Haaga-Helia
ammattikorkeakoulu Oy

VAKOILUOHJELMAT MOBIILILAITTEISSA

Egle Kuivaniemi

Opinnäytetyö
Tietojenkäsittelyn ko.
2016

Haaga-Helia ammattikorkeakoulu Oy

Tiivistelmä

01.05.2016

Tekijä(t)
Kuivaniemi Egle

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Vakoiluohjelmat mobiililaitteissa

Sivu- ja liitesivumäärä
39 + 7

Opinnäytetyön otsikko englanniksi
Spyware in mobile devices

Opinnäytetyön aiheena ovat tunnetuimpien mobiililaitteiden vakoiluohjelmat. Opinnäytetyön teoriaosassa selvitetään mikä on vakoiluohjelma ja mitä se voi saada aikaan mobiililaitteella. Tutkimus sai alkunsa tutkijan omasta mielenkiinnosta aihetta kohtaan. Ajankohtaisuudesta huolimatta mobiililaitteiden vakoiluohjelmista tuntuu olevan saatavilla niukasti tietoa.

Mobiililaitteiden vakoiluohjelmat ovat yleistyvä, mutta vähän tunnustettu ongelma. Tutkijan mielenkiintona oli selvittää aiheesta löytyvän tiedon määrä. Teoriaosuuden tueksi, osana opinnäytetyötä teetettiin internet -kysely 18–55 -vuotiaille, yleisimpien mobiililaitteiden käyttäjille. Kyselyssä selvitettiin mobiililaitteiden käyttöä, yksityisten tietojen jakamista ja asenteita tietoturvariskejä kohtaan. Lisäksi opinnäytetyössä on haastateltu kahta henkilöä, jotka ovat työnsä puolesta tekemisissä mobiililaitteiden ja niiden tietoturvan kanssa.

Opinnäytetyö toteutettiin keväällä 2016. Kysely toteutettiin aikavälillä 26.3–9.4.2016. Vastaajilla oli kaksi viikkoa aikaa vastata kyselyyn. Kyselyyn saatiin yhteensä 42 vastausta. Internet -kyselyn avulla vastauksia saatiin ympäri Suomea.

Tutkimuksen tuloksena havaittiin, että koottua ja kattavaa tietoa aiheesta on hyvin vähän. Painettua tietoa ei aiheesta löytynyt käytännössä ollenkaan. Kyselyn tulosten mukaan mobiililaitteita käytetään päivittäin suuria määriä. Käyttäjät jakavat kuviaan ja henkilötietojaan useissa eri paikoissa. He eivät yleisesti ottaen ole huolissaan tietojensa väärinkäytöstä tai vakoiluohjelmien saamisesta laitteeseensa. Käyttäjät uskoivat tietävänsä vakoiluohjelmista enemmän kuin todellisuudessa tiesivät. Mobiililaitteiden vakoiluohjelmat ovat huomaamattomasti mobiililaitteissa yleistyvä ongelma, jonka riskejä ja haittoja ei vielä juuri tunnisteta.

Asiasanat
Mobiililaite, haittaohjelma, vakoiluohjelma

Haaga-Helia
University of Applied Sciences

Abstract

05.05.2016

Author(s)
Kuivaniemi Egle

Degree programme
Business Information Technology

Report/thesis title
Spyware in mobile devices

Number of pages and appendix pages
39 + 7

The subject of this thesis are the most known spyware programs in mobile devices. The theoretical part of the thesis explains what spyware is and what it can do to a mobile device. The study was initiated due to the researcher's own interest in the issue. Despite the topicality of the subject, there seems to be only little reliable information about spyware in mobile devices.

Mobile Devices spyware is a growing, though insufficiently recognized problem. The study focused on accumulating reputable information as its theoretical background. In support of the theory part, as part of the thesis, the researcher carried out an Internet survey of Finnish people ages between 18 and 55, who used the most common mobile devices. The survey examined the use of mobile devices, private sharing of information and attitudes towards information security risks. In addition, the researcher interviewed two persons who work with mobile devices and their information security.

The research was done during the spring of 2016. The survey was conducted over the period of 26.3-9.4.2016. The persons who answered the survey had two weeks to respond. A total of 42 responses were received. Due to the Internet-based format, responses were received from all over Finland.

As a result of the study, it was revealed that comprehensive knowledge of the subject is very limited. Print-based information was not found practically at all. According to the survey results, mobile devices are being used daily on an intensive level. Users share their photos and personal information in various locations. They are generally not concerned about the misuse of their personal data or getting spyware programs on their devices. The users believed they knew more about spyware than they actually knew. The study concludes that spyware programs in mobile devices are becoming a larger scale problem, which risks and threats are not yet precisely identified.

Keywords
Mobile device, malware, spyware

Sisällys

1 Johdanto

Olet tietämättäsi voinut saada mobiililaitteeseesi jonkin vakoiluohjelman, se on voinut olla laitteellasi jo useamman kuukauden keräten sinusta tietoja. Mobiililaitteiden vakoiluohjelmien olemassaoloa ei juurikaan vielä tunnusteta. Oletettavasti niiden ei vielä uskota olevan kovin vaarallisia tai yleisiä.

Vakoiluohjelmat ovat yksi osa-alue nykyajan haittaohjelmista. Nämä haittaohjelmat keräävät laitteesta ja laitteen käyttäjästä tietoja talteen ja mahdollisesti lähettävät niitä eteenpäin kolmannelle osapuolelle. Vakoiluohjelmat eivät tarvitse tähän käyttäjän suostumusta, vaan suorittavat nämä toiminnot taustalla ilman, että käyttäjä on tietoinen tapahtuneesta.

Opinnäytetyössä pyritään selvittämään mitä tietoa yksityisen käyttäjän tulisi tietää mobiililaitteiden vakoiluohjelmista, kuinka yleisiä nämä ohjelmat ovat, sekä laatia selkokielinen tiivistelmä vakoiluohjelmien vaarallisuudesta. Tavoitteena on myös tutkia, miten hyvin suomalaiset tiedostavat olemassa olevat riskit jokapäiväisessä elämässään mobiililaitteiden kanssa. Teetin suomenkielisen kyselyn, jossa selvitettiin yksityishenkilöiden tietämystä ja asenteita vakoiluohjelmia kohtaan. Kyselyn kohderyhmäksi on rajattu 18–55 vuotiaat asiaan erityisesti etukäteen perehtymättömät henkilöt.

Opinnäytetyön sekä kyselyn tulosten tueksi haastateltiin kahta mobiililaitteiden kanssa tekemisissä olevaa ammattilaista. Myymäläpäällikkö Marko Petäjä on työskennellyt yli viisi vuotta teleoperaattori Elisalla. Toinen haastateltava, Mikael Albrecht, on suomalaisen tietoturvayhtiö F-Securen turvallisuusasiantuntija.

Tutkimus keskittyy kaikista mobiililaitteista ainoastaan älypuhelimiin sekä tablettitietokoneisiin. Työ käsittelee vain yksityisellä henkilöllä, vapaa-ajallaan käytössä olevia mobiililaitteita, sillä työkäytössä olevilla mobiililaitteilla on poikkeavat tietoturvavaatimukset yksityisessä käytössä oleviin verrattuna.

Opinnäytetyö sai alkunsa omasta mielenkiinnostani. Oman osaamisen kehittämisenhalun lisäksi mielenkiintoani nostattivat suomalaisten oletettu vähäinen tieto mobiililaitteiden vakoiluohjelmia kohtaan. Lisäksi oletan, että painettua, tiivistettyä tietoa asiasta olevan melko niukasti saatavilla. Uskon vakoiluohjelmien olevan tulevaisuudessa kasvava ongelma niin yhteiskunnalle kuin yksityishenkilöillekin.

Tutkimuksen teoriaosassa haetaan päällimmäisenä vastauksia seuraaviin kysymyksiin: Mikä on vakoiluohjelma, mitä ne pyrkivät tekemään mobiililaitteissa ja millä tavalla ne to-

teuttavat pyrkimyksensä. Haetaan vastauksia myös kysymyksiin: Kuinka yleisiä nämä ohjelmat ovat, mitä ennaltaehkäisykeinoja on olemassa ja mitä vahinkoa vakoiluohjelmat saavat aikaseksi. Tutkimuksen empiirisessä osassa haetaan vastauksia seuraaviin kysymyksiin: Minkä verran suomalaiset käyttäjät tietävät mobiililaitteiden vakoiluohjelmista ja mitkä ovat heidän asenteet ja kokemukset vakoiluohjelmia kohtaan.

Tutkimuksen tuloksia tulkitaan kolmen eri muuttujan avulla: vastaajien iän, sukupuolen sekä käytössä olevan mobiililaitteen mukaan.

2 Vakoiluohjelmat

Tässä kappaleessa kerrotaan vakoiluohjelmista, tuodaan esille mikä on vakoiluohjelma ja selvitetään sen ominaispiirteitä. Kappale sisältää kaksi haastattelua vakoiluohjelmiin liittyen. Kappaleeseen on lisäksi otettu tueksi tutkimuksessa teetetyn kyselyn tuloksia siltä osin, kun ne pystytään yhdistämään kappaleen teoriaosuutta tukevaksi.

2.1 Virus ja vakoiluohjelma

Vakoiluohjelma on yksi haittaohjelmien alalajeista. Vakoiluohjelma kaappaa koneen tietoja omaan käyttöönsä ja toimii taustalla ilman käyttäjän tietämystä tai suostumusta. Päästyään koneen sisältöön käsiksi, välittää ohjelma nämä tiedot eteenpäin kolmannelle osapuolelle, usein käyttäjän edes huomaamatta asiaa. Viruksesta poiketen vakoiluohjelma ei pyri tekemään suoranaista haittaa itse laitteelle, vaan se keskittyy keräämään tietoa laitteen käyttäjästä.

Vakoiluohjelmia on tiedettävästi esiintynyt vasta noin 20 vuoden ajan. Ensimmäisen kerran tämä ilmiö tuli vastaan vuoden 1995 loppupuolella, kun Microsoftin liikemallista tehtiin pilaa Usenetissä olevassa viestissä. Ensimmäisen viiden vuoden aikana vakoiluohjelmista puhuttiin vakoiluvälineinä, kuten pieninä kameroina. Vuodesta 1999 lähtien on vakoiluohjelmasta puhuttu nykymerkityksen mukaisesti haittaohjelmana Zone Labsin lehdistötiedotteen julkaisun jälkeen. (Lillbacka, 2012 s.30)

Ensimmäinen mobiililaitteesta löytynyt virus, nimeltään Symbian, havaittiin kesäkuussa 2004. Symbian oli tyypillinen päänvaivaa ja tuhoa laitteelle aiheuttava virus, joka ei kuitekaan vakoiluohjelman tapaan pyrkinyt keräämään tietoa käyttäjästään. Aluksi mobiililaitteille tarkoitetut haittaohjelmat olivat lapsen kengissä, eivätkä aiheuttaneet paljoa harmia käyttäjille. Nykyisin virukset ovat monipuolistuneet ja kehittyneet monimutkaisemmiksi aiheuttaen välillä suuriakin huolia mobiililaitteiden käyttäjille. Monipuolistumisen ja mobiililaitteiden yleistymisen myötä on syntynyt laaja, käyttäjistä erilaista dataa keräävä vakoiluohjelmien kirjo. (Kovamäki, 2007)

Nykyään ongelmana ei näytä olevan niinkään vakoiluohjelmien yleisyys, vaan mobiili- ja tablettilaitteiden käyttäjien välinpitämättömyys tietojensa leviämisestä. (Kuvio 1.) Teettämässäni kyselyssä selvästi yli puolet vastaajista kertoivat, ettei eteenpäin jaetun tiedon jääminen ulkopuolisen tahon käyttöön huolestuta heitä. Vastaajien todellinen pelko vakoiluohjelmien olemassaoloon on pelottavan pieni.

Kuvio 1. Kyselyyn vastanneiden mielipide jaetun tiedon uhkasta päätyä vääriin käsiin

2.2 Vakoiluohjelmien monet tavoitteet

Vakoiluohjelmien tavoitteena on hidastaa käyttäjän laitetta, tuoda esille ei-toivottua mainoksia sekä vakoilla käyttäjän verkkokäyttäytymistä. Viime vuosien aikana vakoiluohjelmien määrä on noussut huimasti ja ne yltävätkin pian virusten rinnalle vaaroineen. Identiteettivarkaudet ovat jatkuvasti aiempaa yleisempiä, sillä jo 15 % vakoiluohjelmista pyrkii varastamaan henkilökohtaisia tietoja kuten salasanoja tai vakoilemaan näppäimistön näppäilyjä. Vakoiluohjelmien suurin tehtävä on kuitenkin yhä kaupallisen tarkoituksen puolella, kun ylimääräiset mainokset pomppivat selaimellasi tai sovelluksessasi jatkuvasti.

Ensimmäiset vakoiluohjelmat kaappasivat aikoinaan puhelinlinjoja modeemin välityksellä ja soittivat maksullisiin numeroihin, ja näin ollen aiheuttivat käyttäjälle tämän tietämättä suuria puhelinlaskuja. Näitä vakoiluohjelmia on yhä käytössä, mutta ne alkavat jäädä uusien vakoiluohjelmien jalkoihin kehityksen mennessä eteenpäin. Yhä useammassa asunnossa on myös valmiiksi rakennettuja internet-pistokkeita, joten vanhoja puhelinjohtoja ei enää tarvita.

Hakkereille ehkä toiseksi hyödyllisimmät vakoiluohjelmat kuuluvat ilmiantajien alaluokkaan. Ne keräävät käyttäjän tietämättä tietoja esimerkiksi selatuista sivustoista tai hakukoneissa käytetyistä sanoista. Nämä vakoiluohjelmat keräävät niin sanotusti etukäteistietoa hakkereille, esimerkiksi käyttäjän tietoturvaohjelmistosta, IP-osoitteen tai verkkotunnuksen, joita käyttäen hakkerit pääsevät myöhemmässä vaiheessa syvempiin tietoihin käsiksi.

Troijalaiset ovat yksi pahimmista ja vaarallisimmista viruksista mitä on kehitetty. Virukset yhdistettynä vakoiluohjelmiin saadaan aikaiseksi kaikkein vaarallisimpia vakoiluohjelmia

mitä on tähän päivään mennessä keksitty. Päästyään laitteelle, asentaa vakoiluohjelma troijalaisen sinne. Tämä troijalainen pyrkii puolestaan varastamaan luottamuksellista tietoa, kuten salasanoja tai pankkikorttien tietoja. Näitä vakoiluohjelmia on jo paljon vaikeampi huomata, sillä ne osaavat käyttää hyväkseen yleisimpien ohjelmistojen tietoturva-aukkoja ja näin soluttautua laitteeseen. (Norton)

”Selaimen kotisivua vaihtavat vakoiluohjelmat eivät välttämättä sisällä viruksia tai troijalaisia, mutta ne käyttäytyvät täysin haittaohjelman tavoin. Ne käyttävät hyväksi ohjelmiston heikkouksia ja soluttautuvat tietokoneeseen, kun käyttäjä vierailee verkkosivustossa. Tästä uudesta vakoilu- ja mainosohjelmien versiosta on erityisen hankala päästä eroon, sillä se vaihtaa selaimen kotisivun muokkaamalla tietokoneen rekisteriä. Siksi kotisivun vaihtaminen perinteisin keinoin on mahdotonta. Jotkin näistä vakoiluohjelmista estävät pääsyn määrättyihin verkkosivustoihin. Tunnetuin tämän tyyppinen vakoiluohjelma on CoolWebSearch, joka ohjaa käyttäjät samannimiseen sivustoon, mutta jotkin versiot sisältävät myös troijalaisia. Käyttäjien onkin oltava erityisen valppaita ja muistettava päivittää ohjelmistonsa.” (Norton)

2.3 Mobiililaitteissa olevien vakoiluohjelmien erityispiirteet

Haittaohjelmat mobiililaitteissa, kuten myös tietokoneissa, aiheuttavat yleensä laitteelle ja käyttäjälle ongelmia ja päänvaivaa. Vakoiluohjelmat keräävät ja lähettävät puhelimesta tietoja salaa ja luvattomasti eteenpäin, kasvattavat puhelinlaskuja, valvovat sekä vakoilevat laitteen käyttöä sekä keräävät tallennettuja salasanoja, käyttäjän ottamia valokuvia ja videoita.

> *”Riippuu ohjelman tekijän motiiveista. Kyber-rikolliset haluavat tietoa, jota voidaan muuttaa rahaksi. Kuten esim. luottokorttinumeroita. Valtioiden vakoiluorganisaatiot haluavat salaisia dokumentteja, kommunikaatiota tai mitä tahansa muuta salaista tietoa. Mustasukkaiset puolisot saattavat käyttää vakoilutyökaluja selvittämään onko partneri uskollinen, mikä selviää hyvin viesteistä.” (Albrecht, 2016)*

F-Securen turvallisuuden asiantuntijalta Mikael Albrechtilta kysyttiin haastattelussa, osaisiko hän kertoa mitä kaikkea tietoa vakoiluohjelma kerää mobiililaitteesta. Hän vastasi kolme pääkategoriaa; luottokorttitedot, salaiset dokumentit sekä puolison mobiililaitteen käyttäminen. Luottokorttitietoja käytetään rahan anastamismielessä, salaisia dokumentaatioita vakoiluihin. Puolison vakoilu johtuu puolestaan useimmiten mustasukkaisuudesta.

Osa vakoiluohjelmista osaa käynnistää puhelimen mikrofonin, ja näin ollen nauhoittaa puhelimen ympäriltä kuuluvia ääniä. ”Maailmalla on myynnissä lukuisia vakoiluohjelmia, joiden avulla puhelimen ympäriltä kuuluvia ääniä saadaan tallennettua, viestejä luettua etänä ja seurattua puhelimen sijaintia. Yleensä tällaisia sovelluksia ei asenna puhelimen käyttäjä, vaan joku muu yrittää vaivihkaa saada sellaisen asennettua. Näitä sovelluksia mainostetaan usein ihmisille, jotka ovat esimerkiksi kiinnostuneita puolisonsa yksityiselämästä. Niitä voidaan myös käyttää lastensuojelun nimissä seuraamaan perheen lasten tekemisiä kodin ulkopuolella. Toki ne sopivat myös teollisuusvakoiluun. Näiden sovellusten luokittelussa on hankaluutena, että ne eivät varsinaisesti ole rikollisia tai laittomia, vaikka niiden käyttö muuhun kuin lain rikkomiseen ei olekaan mielekästä.” (Kovamäki, 2007)

Osilla älypuhelimien sovelluksista on käyttäjältä luvan saatuaan lupa käynnistää mobiililaitteen kamera. Esimerkiksi Whatsapp ja Facebook kysyvät sovelluksen asennettua mobiililaitteelle, saako sovellus käyttää myös mobiililaitteen kameraa ja valokuvatiedostoja. Annettuaan luvan sovellukselle, on sen siis käytännössä mahdollista avata mobiililaitteen kamera käyttäjän siitä mitään tietämättä. Julkisuudessa asiaa ei yleisesti tunnisteta, mutta toisaalta voidaan uskoa, että suurimpien sovellusten omistajat eivät riskeeraisi mainettaan käyttämällä luvatta laitteenomistajan yksityisyyttä hyödykseen edellä mainitulla tavalla. Toisaalta taas pienempien ja tuntemattomien sovellusten voidaan olettaa käyttävät kaikki keinot saadakseen sijaa laajasti kilpailluilla sovellusmarkkinoilla.

2.4 Esiintyvyys

Kuvio 2. Vastaajien kokemuksia mobiililaitteiden vakoiluohjelmista sukupuolittain

Teettämässäni kyselyssä selvisi, etteivät vastanneet olleet vielä tähän mennessä vieneet kertaakaan mobiililaitettaan huoltoon vakoiluohjelman takia. (Kuvio 2.) Joko he ovat itse

osanneet hoitaa ongelman, tai sitten heillä ei ole ollut vielä vakoiluohjelmia mobiililaitteillaan.

Haastattelin myös teleoperaattori Elisan myymälässä myymäläpäällikkönä toimivaa Marko Petäjää. Hän on työskennellyt yhtiössä reilut viisi vuotta. Hän osasi kertoa, että mobiililaitteiden virukset ovat yleistymään päin ja lisääntyvät jopa kuukausittain. Petäjä ei varmaksi osannut sanoa miten suuri osa näistä on juuri vakoiluohjelmia, mutta hänen veikkauksensa mukaan noin puolet. Petäjä kertoi, että mobiililaitteita ei tuoda kovinkaan usein huoltoon vakoiluohjelmien takia, sillä asiakkaat ovat alkaneet itseopiskelemaan vakoiluohjelmista ja niistä eroon pääsemistä.

Vaikka asiaa ei Suomessa eikä maailmanlaajuisesti vielä tunnisteta, alkavat vakoilu- ja haittaohjelmat mobiililaitteissa olla todellinen, merkittävä ja eritoten yleistyvä tietoturvaongelma. Mobiililaitteiden haittaohjelmien kohdalla on jo vuonna 2007 havaittu merkittävä nousu verrattuna kyseistä vuotta edeltäviin vuosiin. Jo tuolloin kyettiin ennustamaan, ettei kehitys mobiililaitteiden vakoiluohjelmien osalta ole laantumassa. (Kovamäki, 2007)

Kuvio 3. Vastaajien kokemuksia vakoiluohjelmista sukupuolittain

Teettämässäni kyselyssä selvisi, että suurimmalla osalla vastaajista ei ole vielä kokemusta mobiililaitteiden vakoiluohjelmista. (Kuvio 3.) Suurin osa ei edes tiedä, mikä vakoiluohjelma on. Vajaa kolmasosa vastasi tietävänsä mitä vakoiluohjelma tarkoittaa, kuitenkaan puolet heistä ei osannut nimetä ainuttakaan vakoiluohjelmaa.

2.4.1 Puhelinliittymän vaikutus vakoiluohjelmien esiintyvyyteen

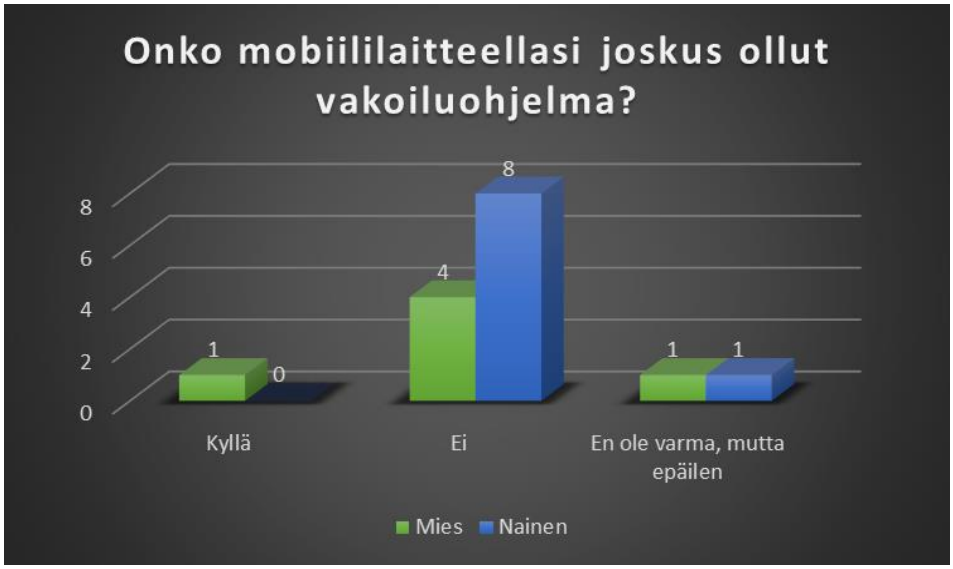
Kyselyn kohdissa 13 ja 14 kysyttiin, minkä teleoperaattorin asiakas vastaaja on.

Kuvio 4. Soneran asiakkaina olevien vastaajien kokemus vakoiluohjelmista sukupuolittain

Soneran asiakkailla ei ole tiedettävästi ollut vakoiluohjelmaa mobiililaitteellaan mutta 10 % vastanneista epäilee sellaisen joskus olleen. (Kuvio 4.)

Kuvio 5. Elisalla asiakkaina olevien vastaajien kokemus vakoiluohjelmista sukupuolittain

Myöskään Elisan asiakkailla ei tiettävästi ole ollut vakoiluohjelmaa mobiililaitteellaan, mutta 12,5 % vastaajista epäilee sellaisen joskus olleen mobiililaitteellaan. (Kuvio 5.)



Kuvio 6. DNA:lla asiakkaina olevien vastaajien kokemus vakoiluohjelmista sukupuolittain

DNA:n asiakkaista 0,7 % vastanneista on ollut vakoiluohjelma mobiililaitteessaan ja 13,3 % vastaajista epäilevät tätä. (Kuvio 6.)

Kuvio 7. Vastaajien kokemus virustorjuntaohjelmista mobiililaitteille sukupuolittain

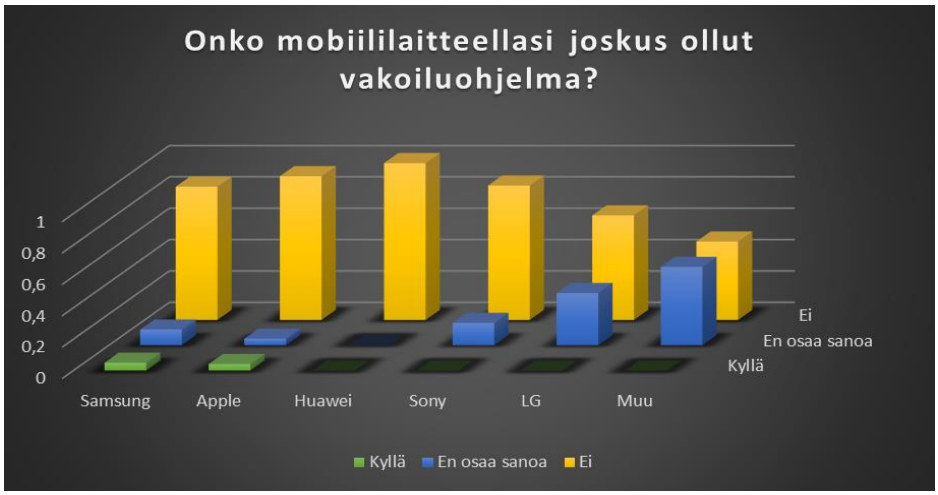
Kyselyni kohdassa 14 kysyttiin, onko vastaaja tilannut teleoperaattoriltaan virustorjuntaohjelman. (Kuvio 7.) 11,9 % vastaajista vastasi, että on tilannut lisäksi myös virustorjuntaohjelman, näistä 60 % vastanneista oli naisia ja loput 40 % miehiä. Kyllä vastanneista 20 % kuului 36–55 – vuotiaiden ikäryhmään ja loput 80 % nuoriin 18–25 – vuotiaisiin. Nuorista kuitenkin vain 16 % vastasi myöntävästi tähän kysymykseen. 26–35 – vuotiaista kukaan ei ollut tilannut mobiililaitteelleen virustorjuntaohjelmaa erikseen. Tarkasteltaessa vain tablet-ti-tietokoneiden käyttäjiä vain 16,7 % vastaajista kertoi tilanneensa erikseen myös virus-torjuntaohjelman.

Kyselyn perusteella teleoperaattorilla ja vakoiluohjelmien saamisella ei olisi suoranaista yhteyttä, vaikkakin vain DNA:n asiakas on vakoiluohjelman mobiililaitteistaan havainnut. Kuitenkin 42 vastaajasta vain yhdellä on ollut mobiililaitteen vakoiluohjelma, joten vakoiluohjelmien tartuntatavasta kyselyn perusteella voi sanoa onko tartunta teleoperaattorista vai käyttäjästä kiinni.

2.4.2 Vaikuttaako laitteen tyyppi yleisyyteen

> *”Applen iOS on käytännössä melkein vapaa haittaohjelmista. Mobiililaitteinen haittaohjelmauhka on lähes täysin Android-laitteiden, kuten esim. Samsungin, ongelma.” (Albrecht, 2016)*

Yksi haastattelukysymykseni oli, että esiintyykö joillain tietyllä tuotemerkillä toisia enemmän vakoiluohjelmia. Albrechtin mukaan iOS olisi käytännössä vielä melkein kokonaan vapaa haittaohjelmista, mobiililaitteiden uhka suuntautuu lähes täysin Android-laitteisiin, kuten Samsungiin.



Kuvio 8. Vastaajien kokemuksia vakoiluohjelmista tuotemerkeittäin jaoteltuina

Kyselyni kohdassa 18 vastaajilta kysyttiin, onko tämän mobiililaitteessa koskaan ollut vakoiluohjelmaa. Tarkastelen vastauksia eri tuotemerkkeihin jaoteltuna. (Kuvio 8.)

Taulukko (Taulukko 1.) auttaa ymmärtämään, miten vastaukset jakaantuivat prosentuaalisesti. Esimerkiksi Huawein käyttäjillä ei oman uskomuksen mukaan ole koskaan ollut vakoiluohjelmaa. Myös Sonyn, LG:n ja muiden tuotemerkkien käyttäjillä vastausprosentti ”kyllä” kohtaan jäi nollaan, mutta näiden merkkien kohdalla vastattiin ”ei” vastauksen li-

säksi myös ”ehkä”. Samsungin ja Applen kohdalla vakoiluohjelmia on ollut jonkin verran, mutta suurin osuus vastausprosenteista sijoittui kuitenkin ”ei” vastaukseen.

Taulukko 1. Vastaukset tuotemerkittäin; uskotko laitteessasi olleen jokin vakoiluohjelma?

Tuotemerkki	**Kyllä**	**Ei**	**En osaa sanoa**
Samsung	5 %	85 %	10 %
Apple	4,2 %	91,6 %	4,2 %
Huawei	0 %	100 %	0 %
Sony	0 %	85,7 %	14,3 %
LG	0 %	66,7 %	33,3 %
Muu	0 %	50 %	50 %

Taulukko 2. Vastaukset käyttöjärjestelmittäin; uskotko laitteessasi olleen jokin vakoiluohjelma?

Käyttöjärjestelmä	Kyllä	Ei	En osaa sanoa
Android	2,5 %	82,5 %	15,0 %
iOS	4,3 %	95,7 %	0 %
Windows	0 %	100 %	0 %

Vertaillessa vastauksia käyttöjärjestelmiin jaoteltuna (Taulukko 2.), on havaittavissa, että iOS:in käyttäjät vastasivat, että olivat ”varmoja” vastauksistaan. Androidin käyttäjistä 15 % vastasi, ettei olisi aivan varma, onko mobiililaitteella joskus ollut vakoiluohjelma, vaiko ei. Windowsin vastausprosentti on 100 % ”ei”, mutta tätä käyttöjärjestelmää vastasi käyttävänsä vain yksi 42:sta.

3 Vakoiluohjelmat mobiililaitteissa

Tässä kappaleessa käydään läpi vakoiluohjelmien leviämistavat, saatavuus, ennaltaehkäisy sekä niiden poistaminen.

3.1 Vakoiluohjelmien leviäminen

Kovamäen (2007) mukaan Mobiilivirukset leviävät yleisimmin mobiililaitteiden välisten Bluetooth-yhteyksien ja MMS-multimediaviestien välityksellä. ”Tämän lisäksi ne voivat levitä SMS-viestien ja saastuneiden Internet- tai WAP-sivujen välityksellä. Kaikille leviämistavoille on yhteistä se, että käyttäjän tarvitsee itse hyväksyä, vastaanottaa tai asentaa virus. Virus pyrkii leviämistavasta riippuen naamioitumaan joksikin hyödylliseksi sovellukseksi, ominaisuudeksi tai esimerkiksi ilmaiseksi soittoääneksi.

Suurin syy mobiilivirusten leviämiseen on kuitenkin mobiililaitteiden käyttäjien tietämättömyys ja välinpitämättömyys. Käyttäjät eivät osaa konfiguroida mobiililaitteidensa Bluetooth-asetuksia ja kokevat mobiilitietoturvasovellusten olevan tarpeettomia. Käytännön esimerkkinä voidaan pitää tilannetta jossa pahaa aavistamaton käyttäjä lataa mobiililaitteeseensa hyödylliseksi ohjelmaksi tai ominaisuudeksi naamioituneen viruksen. Tämän jälkeen virus jää pyörimään moniajoa tukevaan Symbian-käyttöjärjestelmään ja leviää avonaisen Bluetooth-yhteyden kautta muihin suojaamattomiin mobiililaitteisiin. Tämä on erityisen yleinen virusten leviämistapa tilanteissa, joissa on paljon ihmisiä pienessä tilassa, esimerkiksi urheilukisoissa.” (Kovamäki, 2007)

Mobiililaitteen yhdistäminen langattomaan nettiin antaa ulkopuoliselle laitteelle tai henkilölle lähestulkoon vapaat kädet vakoilla mobiililaitetta. Nykyään melkein kaikilla julkisilla paikoilla on tarjota langaton nettiyhteys asiakkailleen. Esimerkiksi kahvilassa yhdistäessä mobiililaitteeseen Wifi-yhteyden, voi viereisessä pöydässä istuva henkilö murtautua laitteeseesi käyttäen samaa Wifi-yhteyttä ja selata kuviasi ja muita tietoja mitä mobiililaitteeseesi olet tallentanut, jopa jokaista toimintoa laitteellasi. Tietysti tämä vaatii jo osaamista ja taitoa, mutta on käytännössä mahdollista. Pankkitunnuksien, sähköpostin tai sosiaalisen median käyttäminen on suositeltavaa vain suojatussa verkossa. (Norton, 2013)

Antamalla luvan ilmaiselle sovellukselle käyttää esimerkiksi mobiililaitteesi kameraa ja kuviasi, voi tämä sovellus luvallisesti tutkia kuvakirjastoasi. On suositeltavaa lukea myös käyttöehdot sovellusta käyttöön ottaessa, jotta tietää mihin antaa sovellukselle luvan**.** Lukematta jättämisellä saattaa ”joutua ”maksamaan” sovelluksista jollakin muulla tavalla, esimerkiksi sallimalla sovelluksen käyttää rajatta yhteyshenkilöluetteloasi tai jopa yksityisiä kuviasi.” (Norton, 2013) Ladattaessa ilmaissovelluksia mobiililaitteelle tai käydessä

epäilyttävillä sivuilla, kuten esimerkiksi internet -sivuilla joista on mahdollista katsoa ilmaiseksi tv -sarjoja, saattaa kylkiäisenä laitteelle latautua myös vakoiluohjelma käyttäjän huomaamatta. Joskus haittaohjelmat latautuvat piilotettuihin tiedostoihin, joita ei aina edes huomaa tai ymmärrä epäillä epäilemään. (Tietoturvapalvelu)

3.1.1 Vakoiluohjelmien saatavuus

Vuonna 2009 julkaistun Yle-uutisten mukaan F-Secure olisi silloin löytänyt jo 26 ohjelmaa internetistä joilla mobiililaitteen käyttöä on mahdollista vakoilla. Vuoteen 2006 mennessä F-Secure ei ollut saanut yhtäkään raporttia mobiililaitteen vakoilusta. Alma Median mukaan lähes kuka tahansa pystyy asentamaan toisen ihmisen älypuhelimeen helpon, halvan ja toimivan vakoiluohjelman. (Yle, 2015) Ohjelmia markkinoidaan huonolla suomenkielellä, mutta niistä käydään keskustelua keskustelupalstoilla jo myös suomeksi.

Mobiililaitteiden vakoiluohjelmat alkavat olla jo kaikkien kuluttajien saatavilla. Pieniä maksuja vastaan internetistä on mahdollista ladata vakoiluohjelmia, joilla voi seurata toisen henkilön mobiililaitteen käyttöä. Aamulehden mukaan vuonna 2008 oli hieman suurempaa maksua vastaan mahdollista ladata myös ohjelma, jonka avulla onnistuisi salakuuntelemaan mobiililaitteen ympärillä olevaa tilaa. Tämän vakoiluohjelman voi ladata vain älypuhelimeen. Ohjelma on mahdollista lähettää puhelimeen joko langattomalla yhteydellä tai asentaa itse omin käsin. Ohjelman asennettua vakoiluohjelma raportoi lataajalle seurattavasta puhelimesta tietoja seuraajan puhelimeen. Vakoillut tiedot on mahdollista käydä tarkistamassa myös palvelimelta web-sivun kautta. (Taloussanomat, 2008)

iSpyoo niminen vakoiluohjelma on mahdollista ladata niin iOS:lle kuin myös Androidillekin. iSpyoo kerää kaikki mahdolliset tiedot mobiililaitteesta yhdelle online-tilille, josta on mahdollisuus päästä myös myöhemmin käsiksi tietoihin, vaikka ne olisi poistettu mobiililaitteesta. iSpyoo kerää muun muassa SMS-viestit, puhelintiedot, GPS-sijainnin, kuvat ja videot, selaimen sivuhistorian ja puhelutallenteet. Lisäksi se tallentaa mobiililaitteen ympärillä olevan äänen ja Whatsapp-viestit online-tilille. Koskematta kohdelaitteeseen on iSpyoon kaukosäädin-ominaisuudella esimerkiksi mahdollista myös lähettää salaisia tekstiviestejä kohdepuhelimesta. Edellä mainittu vakoiluohjelma on mahdollista myös ladata etäältä koskematta kohdelaitteeseen.

Henkilökohtaiseen käyttöön iSpyoo tuntuukin kattavan hyvin käyttötarkoituksensa, sillä se tallentaa kaiken tiedon mobiililaitteesta pysyvästi toiseen paikkaan, vaikka mobiililaitteesta itsestään poistaisi nämä samat tiedot. Usein tätä sovellusta käytetään myös lasten mobiililaitteiden käytön seurantaan, esimerkiksi kun halutaan varmistaa, etteivät lapset surffaile kielletyillä internetsivustoilla. Jos taas ulkopuolinen taho asentaa mobiililaitteeseen käyttä-

jän tiedostamatta tämän sovelluksen vuotaa yksityisen käyttäjän kaikki tieto ulkopuoliselle. Puhelintiedoista näkee, kenen kanssa olet jutellut ja miten kauan, GPS-sijainti kertoo missä mobiililaitteen sijainti on milloinkin. Onlinen tilin omistaja voi katsella vakoiltavasta mobiililaitteista valokuvia ja videoita oman mielen mukaan. Website URL log kertoo vakoilijalle käyttäjän vierailemat sivustot tarjoamalle tälle kaikki URL-osoitteet jotka mobiililaitteesta löytyvät. iSpyoo käynnistää puhelun aikana nauhoittajan ja vakoilija pääsee kuulemaan käyttäjän käymät puhelut, iSpyoo onnistuu nauhoittamaan myös mobiililaitteen ympärillä olevat äänet näin käskettäessä. (Mobilespyonline, 2013)

3.1.2 Vakoiluohjelmat ympäri maailmaa

Yle Uutisten mukaan monet yritykset oletettavasti vakoilevat työntekijöiden (työ)mobiililaitteita, mutta tästä on mahdotonta saada konkreettista näyttöä, sillä yritykset pyrkivät salaamaan tämän viimeiseen asti ylläpitääkseen pörssikurssiaan sekä suojellakseen arvoaan. Suomen lain mukaan vakoiluohjelma itsessään ei ole laiton, mutta sen käyttäminen toisten vakoilemiseen on laitonta. Jos rikosilmoituksessa päädytään vakoiluun, tutkittaisiin tapausta todennäköisesti viestintäsalaisuuden loukkauksena, salakuunteluna ja tietomurtona. Keskusrikospoliisin mukaan ”puhelimien vakoilu on piilorikollisuutta, josta poliisi ei välttämättä koskaan saa tietää. Mobiililaitteiden vakoilusta ei vielä puhuta niin paljoa ääneen kuin esimerkiksi tietokoneiden viruksista, eivätkä käyttäjät osaa epäillä mobiililaitteessaan olevan haittaohjelmaa, vaikka se oudosti toimisikin.” (Yle, 2015)

”Keskusrikospoliisin rikostarkastaja Ari K. Määttä arvioi Aamulehdessä, että jos älypuhelin katsotaan tietojärjestelmäksi, ohjelman saaminen siihen turvajärjestelmän ohi on tietomurto.” (Taloussanomat, 2008)

Yle Uutiset kertoo, että F-Securen mukaan Suomessa etenkin mustasukkaiset ihmiset asentavat puolisonsa mobiililaitteelle vakoiluohjelman. Tietokonevirustutkija Niemelä sanookin, että kännykän vakoilu on perheväkivallan uusi muoto. (Yle, 2015)

Kysyin F-Securen turvallisuuden asiantuntijalta Mikael Albrechtilta haastattelulomakkeella miten yleisiä virukset mobiililaitteissa ovat nykypäivänä, sekä miten suuri osa näistä on vakoiluohjelmia. Albrecht vastasi seuraavasti;

> *”Ensinnäkin, termi virus on pahasti vanhentunut, vaikka suuri osa ihmisistä edelleen käyttää tätä termiä ja ymmärtää mitä se tarkoittaa. Virus oli 80- ja 90-luvuilla erittäin kuvaava termi koska sen ajan haittaohjelmat liittivät itseensä toiseen ohjelmaan ja pääsivät sen kylkijäisenä toisiin järjestelmiin. Nykyajan haittaohjelmat liittävät itseensä toiseen objektin erittäin harvoin.*

Kyseessä on sen sijaan ns. stand-alone malware, siis itsenäisiä ohjelmia jotka tekevät jotain pahaa, kun onnistuvat käynnistymään kohdejärjestelmässä.

Haittaohjelmaongelma on ylivoimaisesti suurin Windows-ympäristössä. F-Securen labra tunnistaa n. 10 000 uutta Windows-haittaohjelmaa joka päivä. Toiseksi eniten haittaohjelmia löytyy Android-ympäristöissä, jossa löytyy alle 1000 uutta haitallista ohjelmaa päivittäin. On kuitenkin huomattava, että kaikki nämä eivät ole uhka Suomalaiselle käyttäjälle. Merkittävä osa näistä on tehty tietylle markkina-alueelle, esim. Kiinaa varten. Applen iOS on melkein kokonaan vapaa haittaohjelmista.

En osaa antaa täsmällisiä lukuja. Eräs haittohjelmakategoria on esim. luottokortteja metsästävä vakoiluohjelma. Mutta nämä ovat yleisiä lähinnä Windows-ympäristöissä.
Mobiililaitteisiin löytyy myös suuri määrä työkaluja, jotka myydään "ylläpitotyökaluna". Nämä mahdollistavat etäyhteyden laitteeseen ja sen seuranta ja tietojen tutkiminen. Tämä on hankala tuotekategoria koska ylläpitotyökalu ei lähtökotaisesti ole paha tai laiton. Nämä muuttuvat pahaksi, kun niitä käytetään väärin, esim. vakoilemalla entistä puolisoaan luurissa. Näitä ei oikein voi estää haittaohjelmatorjunnalla koska itse työkalu ei ole paha tai laiton." (Albrecht, 2016)

Iltasanomien mukaan miljooniin puhelimiin olisi asennettu jo valmiiksi vakoiluohjelma, joka tallentaa käyttäjän näppäilyt, sijaintitiedot ja muun toiminnan reaaliaikaisesti. Sovelluksen on mahdollista lukea tekstiviestit jopa ennen puhelimen käyttäjää. Asiasta ei kerrota puhelimen ostajalle, eikä tätä ohjelmaa voida sulkea pois päältä. Esimerkiksi yhdysvaltalaisen CarrierIQ-yhtiön sovellus tekee tätä, vaikka käyttäjä kieltäisi sen puhelimen asetuksissa. Sovelluskehittäjä Trevor Eckart havaitsi tämän sovelluksen, hänen mukaansa tätä ohjemaa on esiasennettu miljooniin Android käyttöjärjestelmiin sekä Blackberryn ja Nokian älypuhelimiin. Nokian edustaja Mark Durrant kuitenkin kiistää väitteen. Eckhartin mukaan sovellus käynnistyy mobiililaitteessa automaattisesti laitteen käynnistyessä, mutta käyttäjälle ei tule tästä ilmoitusta. HTC-laitteista tätä sovellusta ei edes löydy käynnistä olevien ohjelmien valikosta. Eckhart kertoo, että ohjelma pyörisi aina taustalla eikä sitä saisi koskaan sammutettua. CarrierIQ:n mukaan he myyvät tätä sovellusta operaattoreille ja mobiililaitteiden valmistajille, jotta mobiililaitteiden toimintaa ja operaattoreiden palveluita voitaisiin kehittää. Yhtiö kiistää vakoiluaikeensa, vaikka sovellus selvästi seuraa mobiililaitteen jokaista näppäinlyöntiä, sijaintia sekä viestejä. (Pitkänen, 2011)

Poliiseilla ympäri maailmaa on käytössä sovellus, jolla voidaan tarkkailla hyvin läheisesti monia eri merkkisiä mobiililaitteita. It-viikko Uutisissa kerrotaan Remote Control System (RCS) niminen vakoiluohjelmasta. Se onnistuu tunkeutumaan Androidiin, Blackberryyn, Symbiaan, Microsoftin Windows puhelimeen. ”Edes iPhone ei ole suojassa, joskin se pitää ensin murtaa jailbreakilla.Toinen mahdollisuus RCS:lle tunkeutua iPhoneen on, kun puhelin kytketään tietokoneeseen. Laite toimii myös Windows Mobile -ympäristössä, millä viitattaneen Microsoftin Windows Phonea edeltävään käyttöjärjestelmään. Poliisin tai valtiollisen toimijan pitää ensin tunnistaa kohde ja saastuttaa tämän mobiililaite esimerkiksi juksaamalla tätä vakuuttavalla haittaviestillä. Sen jälkeen RCS pääsee näyttämään kyntensä.

Haittaohjelma osaa muun muassa tallentaa kaikki puhelut, tekstiviestit, chattikeskustelut vaikkapa WhatsAppista ja Skypestä ja varastaa minkä tahansa tiedoston puhelimesta. Kalenteria voidaan vakoilla samoin kuin käyttäjän sijaintia. RCS:n komentaja voi myös ottaa mielivaltaisesti kuvakaappauksia laitteen näytöstä.

Haittaohjelma on koodattu käyttämään maltillisesti kännykän akkua. Sitä ei säästellä kohteliaisuudesta, vaan sen vuoksi, että haittaohjelma olisi paremmin piilossa käyttäjältä.

Vaikka ohjelma on tarkoitettu rikollisten seurantaan, on viitteitä, että sitä on käytetty myös poliittisten kohteiden vakoiluun tietyissä maissa.

Kaspersky listaa blogikirjoituksessaan peräti 326 komento- ja hallintapalvelinta, joilla haittaohjelmaa kaitsetaan eri puolilla maailmaa. Huomattavasti eniten niitä on Yhdysvalloissa, 64 kappaletta, mutta palvelimia löytyi kymmenittäin myös Kazakstanista, Ecuadorista, Isosta-Britanniasta ja Kanadasta. Palvelimien läsnäolo ei kuitenkaan välttämättä tarkoita, että ne olisivat paikallisten viranomaisten käytössä.” (It-viikko, 2014)

Turun Sanomissa kerrotaan toisesta samakaltaisesta vakoiluohjelmasta, nimeltään Toinen FinFisher. Tällä sovelluksella onnistuu myös puhelimen ja mikrofonin käynnistäminen salanauhoituksia varten, Toronton yliopiston Citizen Lab- tutkimuslaitos paljastaa. Tämän vakoiluohjelman on kehittänyt saksalais-brittiläinen Gamma International -yritys. Yrityksen kertoman mukaan se myy sovellusta vain ja ainoastaan hallituksille ja viranomaisille. Todellisuudessa ei ole tietoa miten laajalle tämä vakoiluohjelma on jo levinnyt, tiedettävästi ainakin 14 eri maassa on tätä sovellusta jo käytetty. Koska mobiililaitteissa ei turvallisuusaukkoja ole, on sovellus asennettava mobiililaitteelle huijaamalla käyttäjää. TS-uutisten mukaan Gamman mainosvideoissa tämä tapahtuu esimerkiksi valheellisten päivitysviestien avulla. Haittaohjelma toimii lähes kaikissa kännyköiden käyttöjärjestelmissä, kuten Googlen Androidissa, Apple iOS:ssä ja Nokian Symbianissa. (Lehtonen, 2012)

3.2 Vakoiluohjelmilta suojautuminen ja niiden poistaminen

Virustorjuntayhtiöt ovat kehittäneet myös mobiililaitteille omat palomuurit, ja melkein kaikille tuotemerkeille löytyykin jo oma palomuuri haittaohjelmilta suojautumiseksi.

> *”Nykyisin menee aika hyvin kaupaksi, kun ihmiset tietävät mitä vakoiluohjelmat tekevät.” (Petäjä, 2016)*

Kysyin haastateltavalta Marko Petäjältä, miten virustorjuntaohjelmat menevät kaupaksi Elisalla. Petäjän mukaan virustorjuntaohjelmat menevät nykyään aika hyvin kaupaksi, sillä asiakkaat alkavat olla yhä enemmän ja enemmän perillä mitä vakoiluohjelmat tekevät. Kysyin samaa myös F-Securen asiantuntijalta, Albrecht vastasi seuraavasti:

> *”Haittaohjelmauhka on selvästi pienempi mobiililaitteilla kuin esim. Windowsissa. Torjuntaohjelmien käyttöaste on sen takia myös selvästi alhaisempi. Mobiililaitteiden tiukemmat säännöt appseille hankaloittavat myös haittaohjelmatorjunnan tekoa itse laitteelle. Uskon, että tulevaisuuden torjunta mobiililaitteille tulee olemaan Freedome-tuotteen kaltainen. https://www.f-secure.com/en/web/home_global/freedome Tällainen ratkaisu reitittää verkkoliikenteen VPN-palvelimen kautta ja voi samalla torjua uhkia palvelimen puolelle.” (Albrecht, 2016)*

Ottaen huomioon miten paljon ongelmia mobiililaitteiden vakoiluohjelmat saattavat saada aikaiseksi, on niiltä suojautuminen varsin yksinkertaista. Mobiililaitteisiin on tällä hetkellä saatavilla yhteensä kuusi erilaista tietoturvaohjelmistoa, joista suosituin taitaa olla F-Securen Mobile Anti-Virus. Tietoturvan mukaan F-Securityn tietoturvaohjelmisto tukee S60- ja S80- sarjaa, sekä Windows Mobile 5:a. S60 -sarjan puhelimiin siitä on saatavana kahta eri versiota. Toisessa on mukana ainoastaan virusohjelmisto, mutta toisessa on tämän lisäksi myös palomuuri, joka soveltuu hyvin Bluetooth-yhteyksien tarkkailuun. (Kovamäki, 2007)

”IOS-käyttöjärjestelmä on Applen valmistamissa iPhone-älypuhelimissa ja iPad-taulutietokoneissa. – Emme tietoturvayhtiönä saa kehittää kunnon tietoturvaratkaisua iOS-järjestelmään. Se tarkoittaa katastrofia Applelle**,** Eugene Kaspersky sanoo Register-verkkolehden haastattelussa. Applen iOS on suunniteltu tietoturvallisemmaksi kuin muut käyttöjärjestelmät. Applen ekosysteemi on suljettu ja sen ohjelmia esimerkiksi jaellaan Applen oman sovelluskaupan kautta. Siten ainoa tapa tartuttaa iOS-laite on ujuttaa haittaohjelma laillisten sovellusten koodiin. Sovelluskaupan kautta haittaohjelma leviää nopeasti

”miljooniin tai kymmeniin miljooniin laitteisiin”, Kaspersky pelottelee. Katastrofi syntyy helposti, koska virustorjuntaa ei ole olemassa.

Applen tiukka asenne johtaa Kasperskyn ennusteen mukaan Applen markkinaosuuden laskuun, koska käyttäjät siirtyvät Android-puhelinten käyttäjiksi. Google on antanut tietoturvayhtiöiden kehittää virusohjelmistoja Android-alustaansa. Avoimella käyttöjärjestelmällä on kuitenkin muita käyttöjärjestelmiä synkempi maine tietoturvamarkkinoilla.” (Talous-sanomat, 2012)

Taulukko 3. Luettelo eri sovelluksista turvaamaan eri käyttöjärjestelmiä (AV-Test, 2016)

Android	**iOS**	**Muu**
Alibaba Mobile Security 2.14	Avira Vault	Keeper
Antiy AVL 2.4	Trend Micro Mobile	eWalletGo
Baidu Mobile Security 5.10	iSpyoo	AVG Family Safety
BullGuard Mobile Security 14.0G	Lookout	Best Phone Security
Quick 360 360 Antivirus 2.1	McAfee Mobile Security	Lock & Hide

Erilaisia tietoturvaa suojelevia sovelluksia on kymmeniä erilaisia maailmalla (Taulukko 3.) ja niitä kehitetään koko ajan lisää ja vanhempia paremmiksi. Suomeen näistä ei vielä montakaan ole virrannut käyttöön. Johtuuko sitten suuresta F-Secure virustorjunta – yhtiöstä vai suomalaisten tietämättömyydestä mobiililaitteiden vaarojen suhteen. Kysyin haastateltavalta Petäjältä, että kuinka usein hän työssään kohtaa asiakkaita jotka epäilevät mobiililaitteellaan olevan vakoiluohjelma. Petäjän vastaus oli lyhyt ja ytimekäs;

”Tällaisia tapauksia tulee meidän tietoon erittäin harvoin.” (Petäjä, 2016)

Täytyy kuitenkin muistaa järjenkäyttö ladattaessa sovelluksia mobiililaitteelle, sillä edes parhaimmat palomuurit eivät estä kaikkia sovellusten mukana tulevia vakoiluohjelmia, jos käyttäjä on niille luvan jo antanut. Koskaan ei pidä ladata sellaista sovellusta josta ei varmaksi tiedä, että se on turvallinen. Toinen turvallisuutta lisäävä keino on pitää Bluetooth pois päältä aina kun sitä ei käytä. Bluetoothin välityksellä leviää yhä paljon haittaohjelmia, vaikkei sitä ihan ensimmäiseksi ymmärtäisikään epäillä. ”Edellä mainittujen lisäksi operaattorien tarjoamia esto- ja rajoituspalveluita käyttämällä voidaan rajoittaa mahdollisen haittaohjelman aiheuttamat puhelinlaskut mahdollisimman pieniksi. Niillä voidaan myös estää mobiililaitetta soittamasta ei haluttuihin numeroihin.” (Kovamäki, 2007)
Jos puhelinlasku kasvaa yllättäen tai mobiililaitteessa on outoja ohjelmia tai jokin kuvake välkkyy tekstiviestiä lähettäessä, on siinä todennäköisesti vakoiluohjelma. Virustorjuntaoh-

jelmilla saadaan tämä asia yleensä tarkistettua (Yle, 2015). Aika ajoin on hyvä tarkistaa myös mobiililaitteen tiedostot, ettei niissä näy mitään ylimääräistä.

> *”Valtaosa mobiililaitteiden haittaohjelmista ovat tavallisia appeja jotka huijaavat käyttäjän myöntämään niille oikeuksia luuri tietoihin, kuten esim. kontakteihin. Näiden poisto on yhtä helppoa kun appin poisto. Mutta se ei tietenkään korvaa vakoiluohjelman aiheuttamat vahingot, tietoa on jo vuotanut ja sitä ei saa peruttua.” (Albrecht, 2016)*

Kysyin haastateltavalta vakoiluohjelman poistamisesta mobiililaitteesta, miten se käytännössä onnistuu. Albrecht vastasi, että poistamalla sekä sovelluksen laitteesta että peruuttamalla sovellukselle antamansa luvat asetuksista. Tämä toimenpide ei kuitenkaan korvaa jo aiheutuneita vahinkoja, sillä tietovuoto on saattanut jo tapahtua.

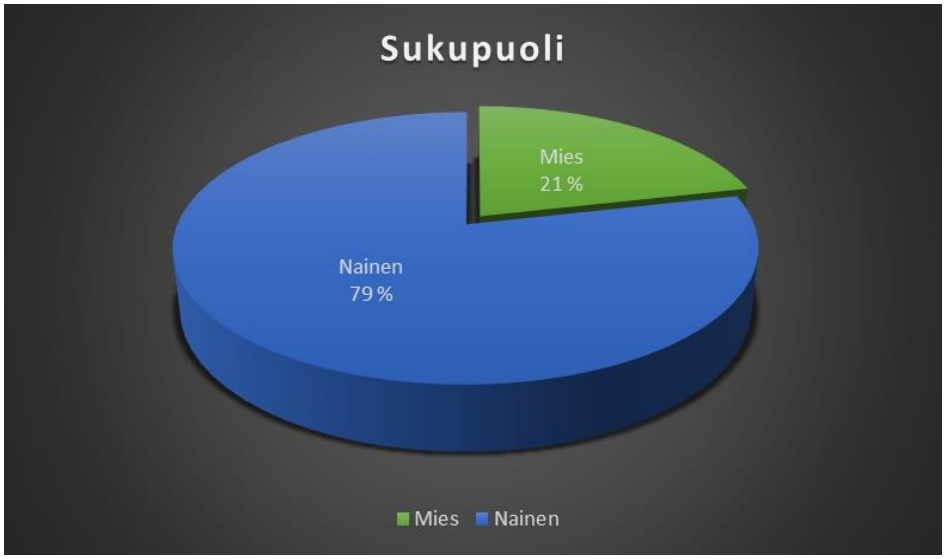
4 Tutkimuksen tulokset

Teetin internetkyselyn, jonka tarkoituksena oli selvittää suomalaisten täysi-ikäisten ihmisten tietämystä vakoiluohjelmista. Kyselyyn vastasi kahden viikon aikana yhteensä 42 ihmistä. Internet-kyselyn avulla vastauksia saatiin ympäri Suomea. Koska kyselyä ”mainostettiin” julkisesti, ei kyselyn vastausprosenttia ole mahdollista laskea. Tarkastelin kyselyn tuloksia kolmesta eri näkökulmasta, sukupuolen, iän sekä mobiililaitteen perusteella. Kyselylomakkeessa on annettu vaihtoehdoiksi neljä eri ikäryhmää, mutta tuloksia tarkastaessa iän mukaan tiivistin nämä kolmeen eri ikäryhmään.

4.1 Vastanneiden taustatiedot

4.1.1 Sukupuoli

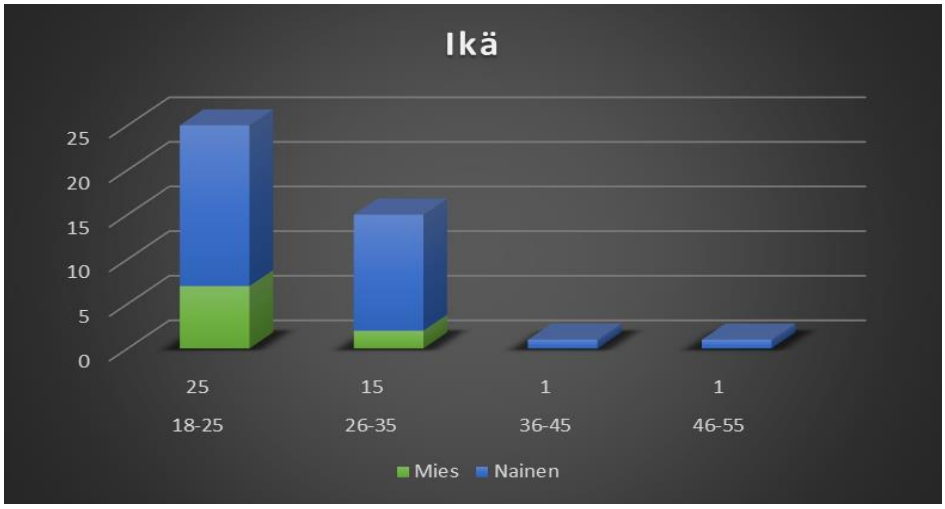
42 vastaajasta 9 oli miehiä ja 33 naisia. (Kuvio 9.)



Kuvio 9. Vastaajien sukupuolijakauma

4.1.2 Ikä

Kyselylomakkeeseen vastausvaihtoehdoiksi oli annettu ikäryhmät 18–25 -vuotiaat, 26–35 –vuotiaat, 36–45 –vuotiaat ja 46–55 –vuotiaat. Yhdistetyt ikäryhmät ovat 18–25 –vuotiaat (25 vastaajaa), 26–35 –vuotiaat (15 vastaajaa) ja 36–55 –vuotiaat (2 vastaajaa). (Kuvio 10.)

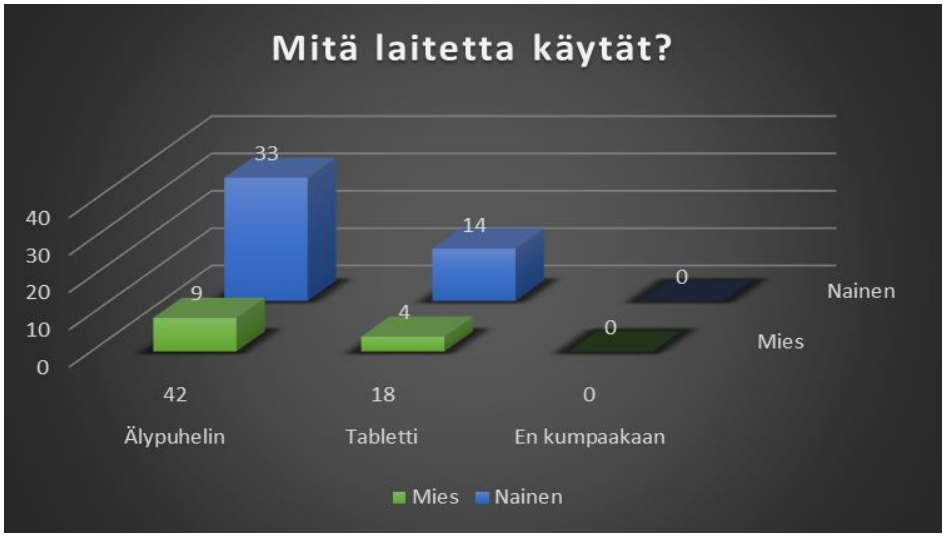


Kuvio 10. Vastaajien ikäryhmät jaoteltuna sukupuolittain ja yhdistettynä

Vastauksia tuli lähinnä nuoremmista ikäryhmistä, 18–25 –ja 26–35 –vuotiaista. Nämä kaksi ikäryhmää yhdistämällä vastaajamäärä oli yhteensä 40 henkilöä, eli 95 % kaikista vastauksista. Kysely ei selvästikään tavoittanut vanhempia sukupolvia niin hyvin kuin nuorempia. Tämä voi johtua hyvin siitä, etteivät iäkkäämmät ihmiset käytä niin paljon mobiililaitteita kuin nuoremmat, mutta myös siitä, että kysely tehtiin netissä eivätkä vanhemmat ihmiset näin ollen löytäneet kyselyä niin herkästi kuin nuoremmat. Tarkoituksenani olikin tutkia enemmän nuorempien sukupolvien tietämystä mobiililaitteiden vakoiluohjelmista, sillä he tiedettävästi myös käyttävät vanhempia ihmisiä enemmän mobiililaitteita ja useampaan tarkoitukseen. Vakoiluohjelmien tartuntariski ei siis lähtökohtaisesti ole niin suuri iäkkäämmällä kuin nuoremmalla sukupolvella. Vanhempien ikäryhmien vastaajia tavoitettiin 2, joka on 5 % kaikista vastauksista.

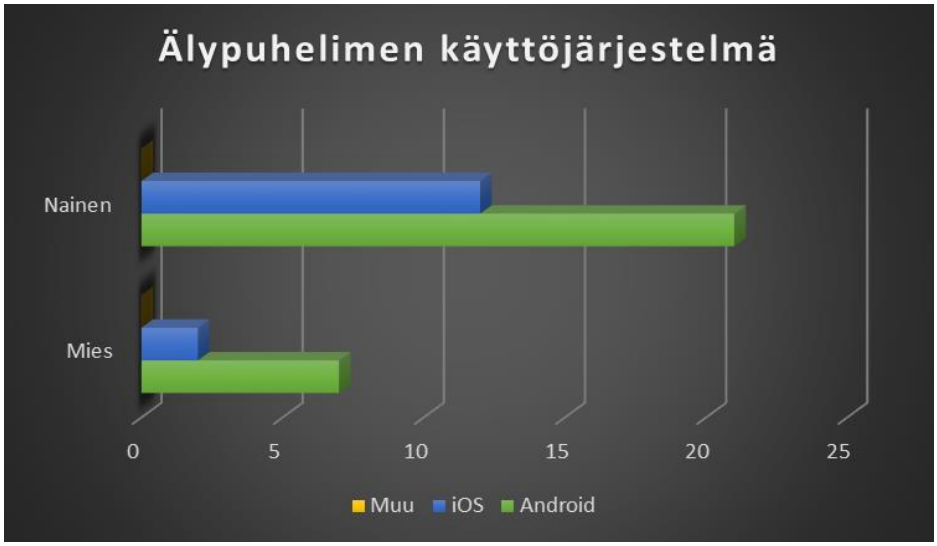
4.2 Mitä laitetta käyttää

Kohdissa kolmesta kahdeksaan pyrin selvittämään mobiililaitteiden käyttöä, mitä, miten ja kuinka paljon päivässä vastaaja käyttää laitetta. Kohdassa kolme vastausvaihtoehtoina oli ”älypuhelin”, ”tabletti” tai ”en käytä kumpaakaan”, näistä oli mahdollista valita useampi. Viimeiseen vaihtoehtoon ei tullut yhtäkään vastausta.



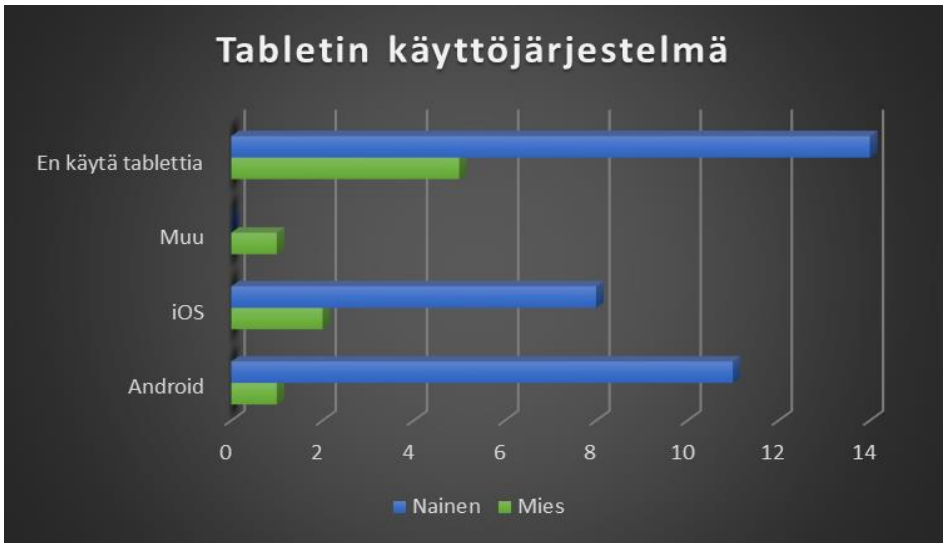
Kuvio 11. Vastaajien käyttämät mobiililaitteet sukupuolittain

Kaikki vastaajat vastasivat käyttävänsä älypuhelinta. Lisäksi 18 henkilöä, 42,9 % vastanneista, kertoivat käyttävänsä myös tablettia. (Kuvio 11.) Miesvastaajista tablettia käytti 44 %, naisista puolestaan 42 %. Ikäjakaumassa on pieniä eroja tabletin käytön suhteen. 18–25 –vuotiaista 52 % vastanneista käyttävät älypuhelimen lisäksi myös tablettia. 26–35 –vuotiaista tabletin käyttäjiä vastanneista oli 26,7 % ja 36–55 –vuotiaista osuus on 50 %. Tablet-tietokoneiden käyttö on selvästi suositumpaa nuorten aikuisten kuin aikuisten tai keski-ikäisten ikäpolvessa.



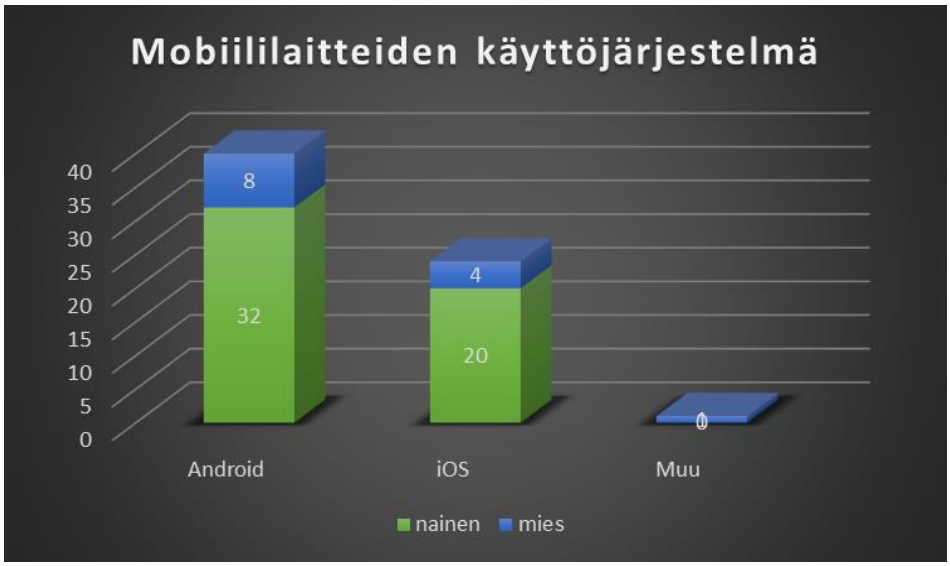
Kuvio 12. Vastaajien älypuhelimien käyttöjärjestelmä sukupuolittain

Selvästi käytetyin käyttöjärjestelmä älypuhelimille oli Android. (Kuvio 12.) Naisvastaajista 63,6 % käyttää Android-älypuhelinta ja loput 36,4 % iOS-älypuhelinta. Miehistä 77,8 % vastaajista käyttävät Androidia ja 22,2 % iOS:ia. Vastausvaihtoehtoina olivat kohdat; Android, iOS, Windows sekä en käytä älypuhelinta.



Kuvio 13. Vastaajien tablettien käyttöjärjestelmät sukupuolittain

Tablet-tietokoneiden kohdalla käyttöjärjestelmien jakauma oli tasainen. (Kuvio 13.) Naisilla Android sai 57,9 % äänistä ja iOS 42,1 % äänistä. Miesvastaajien prosentit jakaantuivat hieman epätasaisemmin; Androidille 25 %, iOS 50 % ja muu (Windows 10) 25 %.



Kuvio 14. Mobiililaitteiden käyttöjärjestelmät

Kaikissa mobiililaitteissa yhteenlaskettuna 61,5 % vastaajista omasi Android -käyttöjärjestelmän, 36,9 % iOS:n ja 1,5 % jonkin muun (yksi Windows) käyttöjärjestelmän. (Kuvio 14.) Ikäryhmittäin vastaukset jakaantuivat niin, että 18–25 –vuotiaista 58,5 %:lla vastaajista oli Android, 39,1 %:lla iOS ja 2,4 %:lla muu (Windows). 26–35 –vuotiailla 71,4 %:lla vastaajista oli Android käytössä ja 28,6 %:lla iOS. 36–55 –vuotiailla 33,3 %:lla vastaajista oli Android ja 66,7 % iOS käytössä. Myös vastaajat jotka käyttävät älypuhelimien lisäksi myös tablet-tietokoneita säännöllisesti suosivat Android käyttöjärjestelmää. Heistä

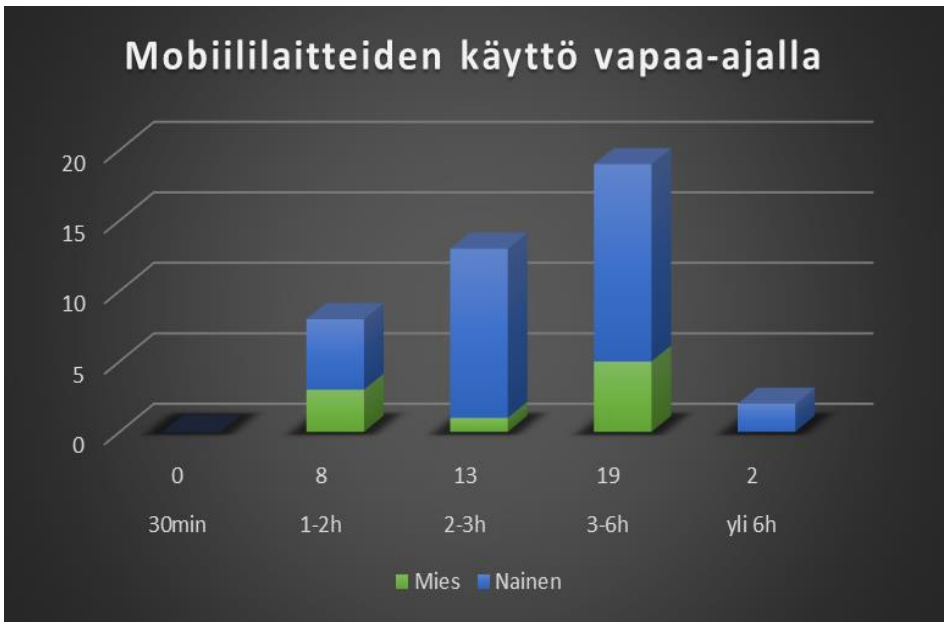
55 %:lla on Android, 42 %:lla iOS ja 3 %:lla Windows käyttöjärjestelmänä mobiililaitteessaan.

Kuvio 15. Vastaajien kokemukset vakoiluohjelmista sukupuolittain käyttöjärjestelmän mukaan

Kyselyyn vastanneiden keskuudessa Android on siis selvästi suositumpi käyttöjärjestelmä. (Kuvio 15.) Android on myös lähtökohtaisesti edullisempi käyttöjärjestelmä kuin iOS. iOS:in valmistajat väittävät, että heidän käyttöjärjestelmälle on lähes mahdotonta asentaa vakoiluohjelmaa. 42 vastaajasta kuitenkin yhdellä on kokemusta myös iOS- pohjaisella käyttöjärjestelmällä olevasta vakoiluohjelmasta. iOS- pohjaisiin käyttöjärjestelmiin ei vielä ole kehitetty virustorjuntaohjelmaa.

Kyselyn kohdassa 18 kysyttiin vastaajilta, onko heidän mobiililaitteellaan ollut joskus vakoiluohjelma. Tuloksia tarkasteltaessa käyttöjärjestelmiin jaoteltuna selvisi, että 85,7 % ”en ole varma” kohdan valinneista käyttää Android käyttöjärjestelmää. Vastausten perusteella Androidia käyttävät henkilöt eivät erota vakoiluohjelmaa mobiililaitteissaan yhtä helposti kuin iOS-laitteiden käyttäjät.

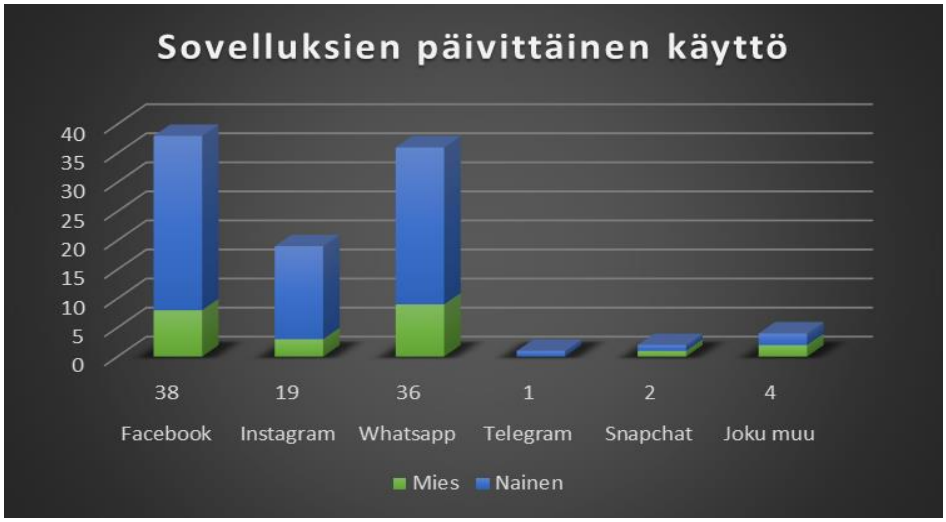
4.3 Internetin käyttö



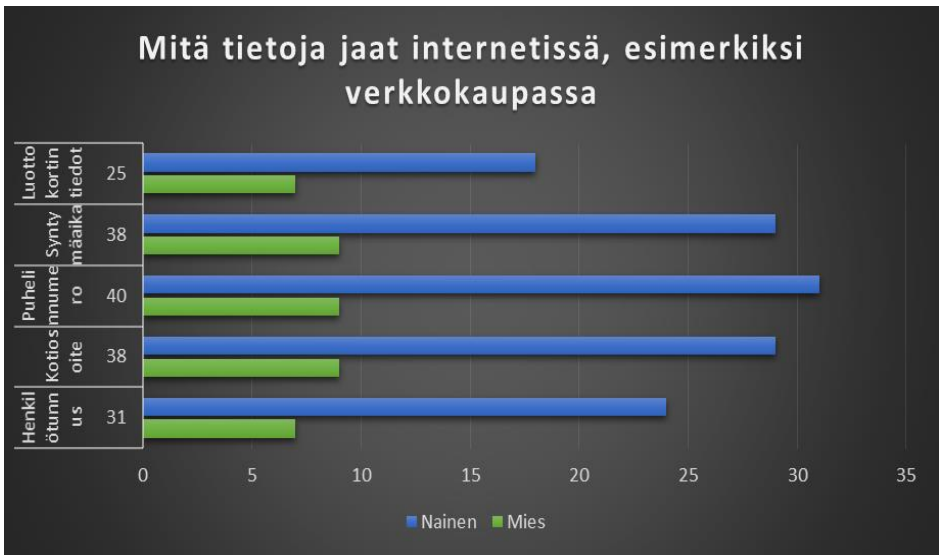
Kuvio 16. Vastaajien mobiililaitteiden käyttö vapaa-ajalla sukupuolittain ja yhdistettynä

Kaikista vastaajista jopa 45,2 % käyttävät mobiililaitteitaan vuorokaudessa 3-6 tuntia. 31,0 % arvioi käyttävänsä 2-3 tuntia vuorokaudesta mobiililaitteitaan ja 19 % vastaajista vastasi käyttävänsä 1-2 tuntia vuorokaudesta. Kukaan ei vastannut käyttävänsä vain 30 minuuttia vuorokaudessa ja vain 4,7 % vastasi viettävänsä aikaa päivästään mobiililaitteita näpertäen yli 6 tuntia vuorokaudestaan. (Kuvio 16.) Miehistä 33,3 % vastasi viettävänsä 1-2 tuntia vuorokaudestaan mobiililaitteessaan, 11,1 % vastasi 2-3 tuntia ja 55,6 % vastasivat 3-6 tuntia. Naisista 15,2 % vastasi 1-2 tuntia, 36,4 % vastasi 2-3 tuntia, 42,4 % vastasi 3-6 tuntia ja 6,1 % yli 6 tuntia.

18–25 –vuotiaiden vastauksista 16 % vastasi 1-2 tuntia vuorokaudessa, 24 % vastaajista valitsi 2-3 tuntia, 56 % valitsi 3-6 tuntia ja 4 % vastasi yli 6 tuntia. 26–35 –vuotiaiden vastaukset jakaantuivat seuraavasti; 26,7 % 1-2 tuntia, 40 % 2-3 tuntia, 26,7 % 3-6 tuntia ja 6,7 % yli 6 tuntia. 36–55 –vuotiaista 50 % käyttää mobiililaitettaan 2-3 tuntia vuorokaudessa ja toinen 50 % 3-6 tuntia. Tarkastelemalla pelkästään tablet-tietokoneiden käyttäjien vastauksia 44,4 % vastaajista käyttävät laitetta vapaa-ajallaan vuorokaudessa noin 3-6 tuntia, 33,3 % vastasivat 2-3 tuntia ja 1-2 tuntia ja yli 6 tuntia saivat molemmat 11,1 % vastauksista. Pelkästään älypuhelimien vastaajien käyttämä aika vuorokaudesta jakaantui aika samassa suhteessa, 45,2 % vastasi käyttävänsä 3-6 tuntia vuorokaudesta, 31,0 % vastasi 2-3 tuntia, 19,1 % vastasi 1-2 tuntia ja 4,8 % vastasi yli 6 tuntia vuorokaudessa.



Kuvio 17. Vastaajien sovelluksien käyttö päivittäin mobiililaitteella sukupuolittain ja yhdistettynä



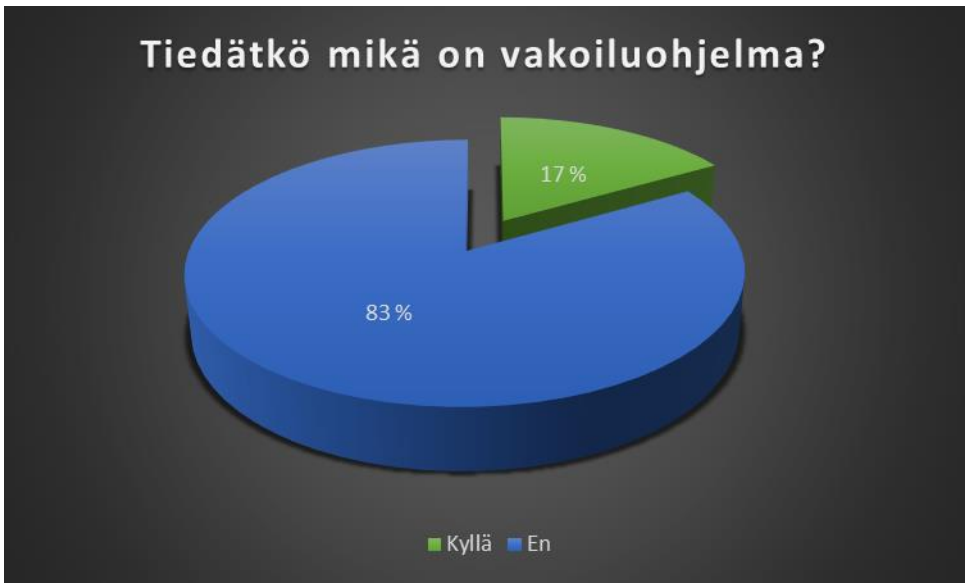
Kuvio 18. Vastaajien tietojen jakaminen internetissä sukupuolittain

Kyselyn kohdissa yhdeksästä yhteentoista selvisi, että suosituimmat sovellukset niin naisille kuin miehillekin ovat Facebook ja Whatsapp, kolmantena oli Instagram. (Kuvio 17.) Kohdassa yhdeksän selvitettiin, mitä tietoja vastaajat jakaisivat internetissä, lähtökohtaisesti tietosuojatuilla sivustoilla (kuvat pois lukien). Vain yksi vastaajista vastasi, ettei jakaisi omia kuviaan internetiin. 95,2 % vastanneista vastasi jakavansa puhelinnumeronsa internetissä, esimerkiksi verkkokaupassa. Syntymäaika sekä kotiosoite saivat melkein yhtä isot kannatukset vastausprosentilla 90,5. Kuitenkaan henkilötunnusta ei yhtä uskaliaasti jaeta (70,8 %) puhumattakaan luottokortin numerosta (59,5 %). (Kuvio 18.) Vastauksista selvisi, että näitä tietoja lähetellään myös mobiililaitteiden sovelluksien välityksellä, kuitenkin pyritään välttämään henkilötunnuksen ja luottokortin tietojen kirjoittamista sovelluksiin. Miehistä lähes jokainen jakaa tietojaan esimerkiksi verkkokaupassa, mutta naiset

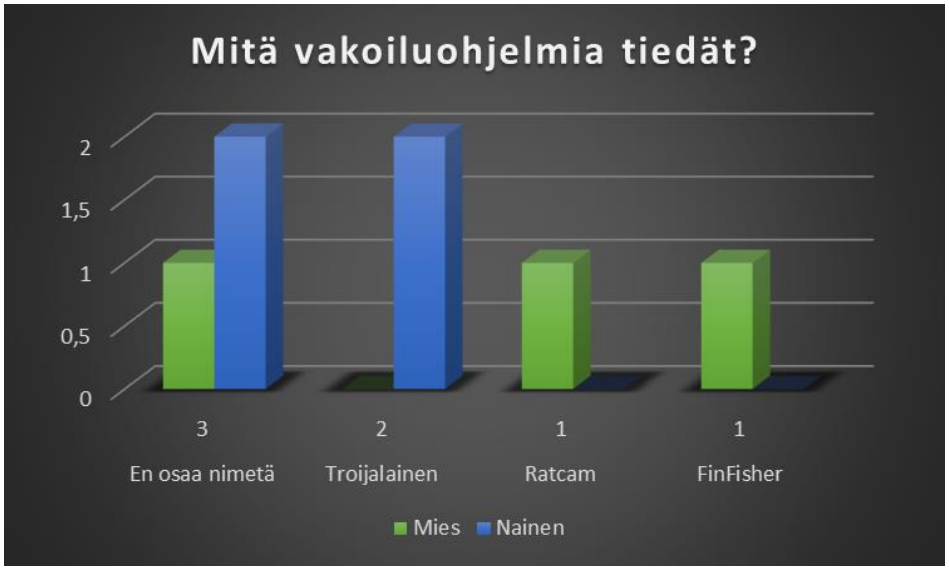
(54,5 %) jakavat miehiä (77,8 %) selvästi harvemmin luottokorttinsa tietoja internetissä. 18–25 – vuotiaat jakavat pääasiassa tasaisesti kaikkia tietojaan internetissä, mutta vähiten kuitenkin luottokorttinsa tietoja (64 %) ja toiseksi vähiten henkilötunnustaan (74 %). 26–35 –vuotiaiden vastauksista selvisi, että he jakavat tasaisesti (80 %) muita tietojaan internetissä, mutta luottokortin tietoja luovutetaan paljon vähemmän (46,7 %) kuin muita tietoja. 36–55 –vuotiaat jakavat kaikkia tietojaan tasaisesti. Tarkasteltaessa pelkästään älypuhelimen käyttäjiä huomasi myös tässä selvän eron luottokortti tietojen jakamisen suhteen (59,5 %), toiseksi vähiten älypuhelimen käyttäjät vastausvaihtoehdoista jakavat henkilötunnusta internetissä (73,8 %). Tarkasteluteltaessa tablet-tietokoneiden käyttäjiä, ei niin selvää eroa huomannut, joskin henkilötunnuksia (66,7 %) jaetaan vähemmän kuin luottokortin tietoja (72,2 %).

4.4 Tietämys vakoiluohjelmista

Kohdassa 16 vastaajilta kysyttiin, tietävätkö he mikä vakoiluohjelma on. 83 % vastanneista ei tiedä mikä vakoiluohjelma on tai mitä sellainen tekee. Vain 17 % kaikista vastanneista tiesi valita kyllä – vaihtoehdon. (Kuvio 19.) Näistä vastaajista oli 57,1 % naisia ja 42,9 % miehiä. Ikäryhmittäin jaoteltuna kaikkein eniten kyllä – vastauksia tuli 18–25 – vuotiaiden joukosta. Tämän ikäisistä vastaajista 24 % oli vastannut tietävänsä, mikä vakoiluohjelma on. 26–35 – vuotiaiden joukosta vain 6,7 % tiesi vakoiluohjelman etukäteen ja 36–55 – vuotiaiden vastauksiin ei tullut yhtäkään kyllä -vastausta. Vertaillessa tablet-tietokoneiden ja älypuhelimien käyttäjien vastauksia eroa ei ollut lainkaan. Molemmissa ryhmissä 83,3 % vastaajista ei tiennyt vakoiluohjelmia.



Kuvio 19. Vastaajien tietämys vakoiluohjelmasta



Kuvio 20. Vastaajien tiedot vakoiluohjelmista sukupuolittain

42 vastaajasta yhteensä neljä, 9,5 %, osasi nimetä vakoiluohjelman nimeltä. Näistä vastaajista 50 % oli miehiä ja 50 % naisia. Nämä kaikki vastaukset on annettu 18–25 – vuotiaiden ikäryhmän joukosta. Seitsemän kuitenkin vastasi, että tietää, muttei osaa nimeltä yhtäkään. Näistä vastauksista 85,7 % oli 18–25 – vuotiaiden joukosta ja loput 14,3 % 26–35 – vuotiaiden joukosta. 42,9 % tietävistä käyttävät myös tablet-tietokonetta älypuhelimen lisäksi. (Kuvio 20.)

Vastaajista hyvin pieni osuus tiesi vakoiluohjelmista ennen kyselyyn vastaamista ja vielä pienempi osuus osaa nimetä eri vakoiluohjelmia. Vakoiluohjelmista tietävien joukko koostuu lähinnä nuoremmasta ikäpolvesta. Vanhemmat ihmiset eivät luultavimmin ole edes kuulleet vakoiluohjelmien olemassa olosta mobiililaitteissa. Toisaalta vanhemmat henkilöt eivät myöskään käytä mobiililaitteita yhtä ahkerasti ja monipuolisesti kuin nuoremmat, josta johtuen uhka ei tunnu niin suurelta vanhempien kuin nuorempien kohdalla. Selvää eroa ei sukupuolten väliltä löytynyt, tietämys molemmilla ryhmillä on yhtä vähäinen. Suuri osa jakaa henkilökohtaisia tietojaan ympäri internetiä tietämättä mikromaailman jatkuvista vaaroista ja uhista.

4.4.1 Ajatukset vakoiluohjelmista

Kuvio 21. Vastaajien ajatuksia vakoiluohjelmista mobiililaitteissa sukupuolittain

Kohdassa 17 kysyttiin vastaajilta pelkäävätkö he saavansa joskus vakoiluohjelman mobiililaitteeseensa. 59,9 % kaikista vastaajista vastasi ettei pelkää saavansa vakoiluohjelmaa. (Kuvio 21.) Miehistä kielteisesti vastasi 66,7 % ja naisista 57,6 %. Ikäryhmittäin kielteisiä vastauskia tuli 18-25 – vuotiaissa 64,0 %, 26-35 – vuotiaissa 53,3 % ja 36-55 – vuotiaissa jakauma oli tasan puoliksi, eli 50 %. Pelkästään tablet-tietokoneiden käyttäjistä 66,7 % vastasi, ettei pelkää vakoiluohjelmatartuntaa, kun taas älypuhelmien käyttäjistä 59,5 % vastasi, ettei pelkää vakoiluohjelman saamista omaan mobiililaitteelleensa.

Kuvio 22. Vastaajien ajatuksia mitä tekisi vakoiluohjelmalle mobiililaitteella

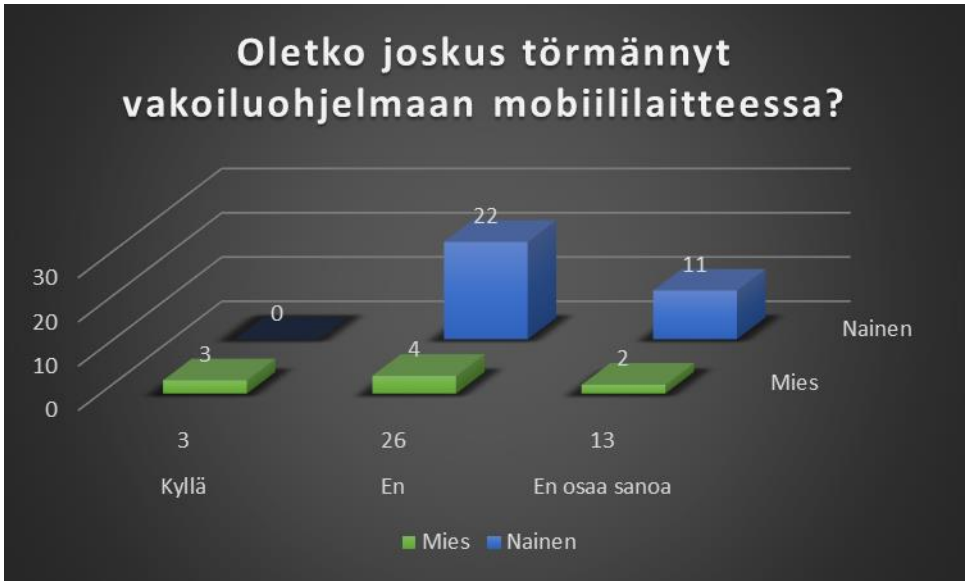
Kohdassa 19 selviteltiin vastaajien toimenpiteitä mahdollisen vakoiluohjelman tullessa omaan mobiililaitteeseen. Vastauskenttä oli jätetty avoimeksi ja vastaajat saivat vastata omin sanoin. (Kuvio 22.) Kaikista vastaajista 14,9 % vastasi ettei tietäisi mitä tekisi. 38,3 % vastasi vievänsä mobiililaitteen huoltoon. 10,6 % vastanneista kertoi nollaavansa/tyhjentävänsä laitteen (ja samalla pääsevänsä eroon vakoiluohjelmasta). 8,5 % vastasi poistavansa vakoiluohjelman itse jotenkin, tietoa poistosta ei kylläkään ollut vielä etukäteen, 14,7 % aikoi ensin kysyä tutulta tai mieheltä apua, ennen huoltoon viemistä tai omatoimista vakoiluohjelman poistamista. Yhteensä 25,5 % antoivat vastauksia, joista ei sillä hetkellä olisi todellisuudessa hyötyä.

Kuvio 23. Vastauksia toimenpiteistä vakoiluohjelmalle mobiililaitteella sukupuolittain

Lähemmin tarkasteltuna ja sukupuolittain jaoteltuna miehistä 55,6 % tietäisi miten päästä itse eroon vakoiluohjelmasta. Vastausten mukaan 22,2 % vastanneiden toimeenpiteet eivät johtaisi mihinkään suuntaan ja loput 22,2 % veisi laitteen kolmannen osapuolen huolenaiheeksi. (Kuvio 23.) Naisista enemmistö, 51,5 % veisi laitteen suoraan huoltoon, 21,2 % vastasi ettei tietäisi mitä tekisi siinä tilanteessa ja 27,3 % vastasi kysyvänsä tutultaan apua ja koittavansa pärjätä ilman huoltoa poistamisen kanssa. Kukaan naispuolisista vastaajista ei kuitenkaan suoralta kädeltä tiennyt miten vakoiluohjelman saisi poistettua. Ikäryhmittäin tarkasteltuna 18-25 – vuotiaista 11,5 % ja 26-35 – vuotiaista 12,5 % tiesi miten pääsisi eroon vakoiluohjelmasta, 36-55 – vuotiaista tämä vastausprosentti pysyi nollassa. Tästä vanhimmasta ikäluokasta 100 % vastanneista vastasi vievänsä laitteen siinä tilanteessa huoltoon. 18-25 – vuotiaista 34,6 % ja 26-35 – vuotiaista 43,8 % vastasi vievänsä laitteen huoltoon. Kaiken kaikkiaan 18-25 – vuotiaista 30,8 % ja 26-35 – vuotiaista 25 % vastanneista ei joko tietäisi tai tekemä toimenpide ei

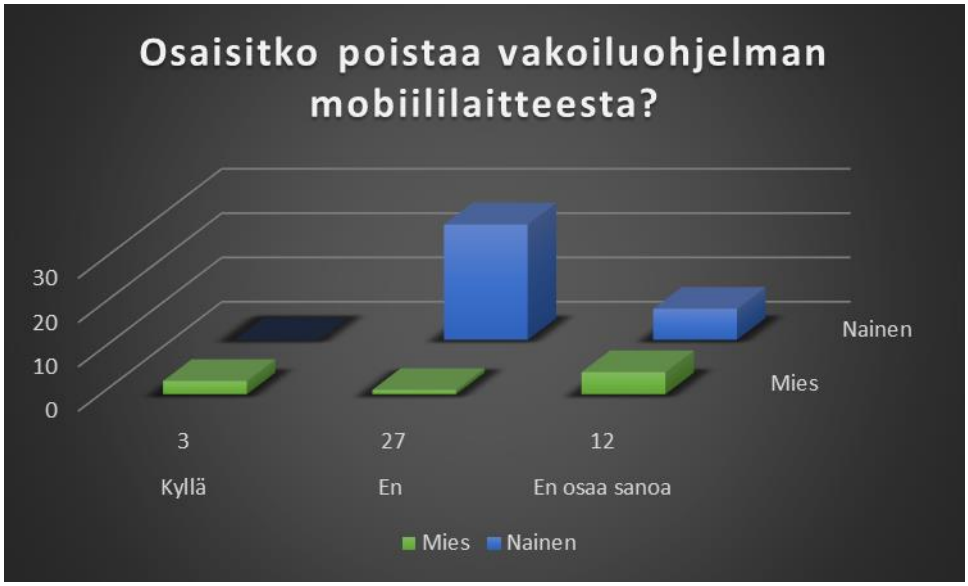
auttaisi tilannetta yhtään. Tablettietokoneiden käyttäjien vastauksista 26,3 % oli hyödyttömiä vakoiluohjelman vallatessa laitteen, näistä käyttäjistä 36,8 % vastasi vievänsä laitteensa huoltoon. Kaiken kaikkiaan huoltoon vieminen sai kaikkein eniten kannatusta kaikissa eri jaotteluryhmissä, vastaajat ovat siis ennemmin valmiit maksamaan vakoiluohjelman poistamisesta, kuin selvittämään itse (ja poistamaan) miten tästä haittaohjelmasta pääsisi eroon.

4.4.2 Poistamis- ja asentamistaidot



Kuvio 24. Vastaajien kokemus vakoiluohjelmista sukupuolittain

Kohdassa 20 kysyttiin oliko vastaaja törmännyt elämänsä aikana mobiililaitteen vakoiluohjelmaan. Kaikista vastanneista 61,9 % vastasi kieltävästi ja 31,0 % ettei olisi aivan varma. (Kuvio 24.) Pelkästään miehistä kielteisiä vastauksia antoi 44,4 % ja epävarmoja 22,2 %. Naisista taas kielteisen vastauksen antoi 66,7 %, epävarman 33,3 % ja myöntävän ei yksikään. Ikäryhmittäin kielteisen vastauksen 18-25 – vuotiaiden joukossa antoi 52,0 % ja epävarman 36,0 %, 26-35 – vuotiaista kukaan ei vastanut myöntävästi, kielteisesti vastasi 73,3 % ja epävarmasti 26,7 % ja 36-55 – vuotiaista 100% vastasi ettei olisi ennen törmännyt mobiililaitteen vakoiluohjelmaan. Tablet- tietokoneiden käyttäjistä 66,7 % vastasi kielteisesti, loput 16,7 % vastasi epävarma ja toiset 16,7 % myöntävästi. Tablet- tietokoneiden käyttäjistä nuoret miehet, 18-25 – vuotiaat ovat siis elämänsä aikana törmänneet joskus vakoiluohjelmaan mobiililaitteessa.



Kuvio 25. Vastaajien tietämys vakoiluohjelmista sukupuolittain

Kohdissa 20 ja 21 kysyttiin osaisiko vastaaja poistaa tai asentaa vakoiluohjelman mobiililaitteesta. Kaikista vastanneista kaikkiaan 64,3 % vastasi ettei osaisi poistaa, vain 7,1 % vastasi osaavansa, loput eivät olleet varmoja. (Kuvio 25.) Naisista kukaan ei vastannut osaavansa poistaa vakoiluohjelmaa mobiililaitteesta (selvisi edellisessä kohdassa jo). Naisista kuitenkin 28,6 % epäilee osaavansa. 18 -25 – vuotiaista 12 % vastasi tietävänsä miten vakoiluohjelma poistettaisiin ja 26-35 – ja 36-55 – vuotiaista kukaan ei vastannut onnistuvansa siinä. Tarkastelemalla tablet- tietokoneiden käyttäjien antamia vastauksia, niin heistä 11,1 % osaisi poistaa vakoiluohjelman mobiililaitteestaan ja 27,8 % vastasi, ettei ole ihan varma.

Kuvio 26. Vastaajien tietämys vakoiluohjelmista sukupuolittain

Kaikista vastanneista ”en osaa asentaa” vastasi 72,6 %, 19,0 % vastanneista ei osannut sanoa ja vain 4,8 % vastasi osaavansa asentaa vakoiluohjelman mobiililaitteelle. (Kuvio 26.) Miehistä 22,2 % vastasi osaavansa asentaa haittaohjelman, toiset 22,2 % vastasi ettei ole ihan varma ja loput 55,6 % etteivät osaa. Naisten vastaukset taas jakaantuivat niin, että 81,8 % vastanneista vastasi ettei osaa ja loput 18,2 % eivät olleet aivan varmoja osaisivatko. Ikäjakaumittain tarkasteltuna vain nuorimmassa joukossa 8,0 % vastasi osaavansa asentaa vakoiluohjelman mobiililaitteelle. Muuten suosituin vastaus oli ”en osaa asentaa” jokaisessa kategoriassa, 18-25 –vuotiaista 72,0 %, 26-35- vuotiaista 80,0 % ja 36-55 –vuotiaista 100% vastasi kielteisesti ja loput vastaajista olivat valinneet kohdan ”en osaa sanoa”. Vain tablet-tietokoneita käyttäneistä vastaajista 5,6 % vastasi hallitsevansa asennustaidot, 33,3 % ei ollut varma ja loput 61,1 % sanoivat suoraan etteivät osaa asentaa.

4.4.3 Mitä haluaisit oppia lisää vakoiluohjelmista

Kuvio 27. Vastaajien kiinnostuneisuus vakoiluohjelmista sukupuolittain

Kyselyn viimeisessä kohdassa, eli 23, kysyttiin haluaisiko vastaaja oppia lisää mobiililaitteiden vakoiluohjelmista. (Kuvio 27.) 54,8 % kaikista vastaajista vastasi ettei osaa sanoa, 21,4 % vastasi ettei lisäopiskelu kiinnosta ja 23,8 % vastasi haluavansa oppia lisää. Miehistä ei kukaan osoittanut kiinnostusta lisäopiskelulle, mutta 44,4 % vastaajista vastasi että on kahden vaiheilla. Nuorimmasta ikäryhmästä vain 16,0 % vastasi haluavansa oppia lisää, keskimmäisestä ikäryhmästä vastasi näin 33,3 % ja vanhimmasta ikäryhmästä 50,0 % vastasi näin. Vanhimmasta ikäryhmästä kukaan ei vastannut kieltävästi tähän kysymykseen, mutta keskimmäisestä ikäryhmästä vastasi 26,7 % ja nuorimmasta näin vastasi 20,0 %. Suurimman suosion vei taas ”en osaa sanoa”-

vastaus saanen nuorimmasta ikäryhmästä jopa 64 % äänistä, keskimmäisestä ikäryhmästä 40,0 % ja vanhimmasta ikäryhmästä 50,0 %. Tarkasteltaessa ainoastaan tablet-tietokoneiden käyttäjiä lisäopiskelu sai kannatusta vain 11,1 % vastauksista ja ”en osaa sanoa” taas enemmistön, eli 61,1 %.

Kuvio 28. Vastaajien kiinnostuneisuus vakoiluohjelmista

Viimeiseen kysymykseen ”kyllä” vastanneita pyydettiin vastaamaan vielä lisäkysymykseen ”Mitä haluaisit oppia lisää?”. (Kuvio 28.) Vastaukset eivät sisällä lainkaan miesten näkökulmia, sillä yksikään miehistä ei kokenut haluavansa lisää opetusta aiheesta. 54,0 % vastaajista haluaisia oppia tunnistamaan vakoiluohjelman. Seuraavana jonossa tulivat 15 %:lla ennaltaehkäisy ja tieto miten vakoiluohjelman voi poistaa. Kolmansina kahdeksalla prosentilla kannatusta sai ”oppisi tietämään mitä vakoiluohjelma tekee” ja ”kaikki mahdolliden”. ”Tunnistaminen” vastanneista 57,1 % oli 18-25 – vuotiaita, 28,6 % oli 26-35 – vuotiaita ja 14,3 % vastanneista oli 35-55 – vuotiaita. Tablet-tietokoneiden käyttäjistä vain 11,1 % vastasi tähän kysymykseen, mutta vastaus oli yhtenevä ja he haluaisivat oppia lisää juuri nimenomaan mobiililaitteiden vakoiluohjelmien tunnistamista. ”Poistaminen” vastanneista 100 % oli 18-25 – vuotiaita. 26-35 – vuotiaat vastasivat myös ”ennaltaehkäisy” sekä ”kaiken mahdollisen”.

5 Pohdinta

5.1 Tutkimustulosten tarkastelua

Tutkimuksen kyselytulosten mukaan vastaajien mobiililaitteiden käyttö oli yleisesti ottaen runsasta. Hieman iäkkäämmät vastaajat käyttivät mobiililaitettaan hieman maltillisemmin ja suhtautuivat käyttöön hieman varauksellisemmin. Nuoret, etupäässä naiset, käyttävät mobiililaiteitta päivittäin hurjia määriä. Runsaasta käytöstä huolimatta, kuten oletettua, käyttäjät eivät tunnu uskovan vakoiluohjelmien todelliseen vaaraan. Mobiililaitteiden käyttö nettikauppoineen ja sosiaalisine medioineen on niin arkipäiväistä, että henkilökohtaisten tietojen jakamisessa ei nähdä juurikaan riskejä. Tämä voi juontaa juurensa mobiililaitteiden lyhyeen historiaan. Valtaosan vastaajista ensimmäinen puhelin on ollut täysin haittaohjelmista vapaa laite, jolla joko soitettiin, lähetettiin tekstiviestejä tai pelattiin matopeliä. He ovat sukupolvea, jotka ovat tottuneet siihen, että viruksia ja haittaohjelmia esiintyy ainoastaan tietokoneissa. Tulevaisuudessa asia voi olla toisin; uuden sukupolven ensimmäinen puhelin on todennäköisesti älypuhelin. Tuloksista voi myös päätellä, että ihmiset uskovat tietävänsä mobiililaitteiden turvallisesta käytöstä enemmän kuin todellisuudessa tietävätkään. Tämä voi olla hyvinkin vaarallinen tekijä, sillä vakoiluohjelmat kehittyvät jatkuvasti ovelimmiksi ja vaikeammaksi havaita. Tiivistettynä voi todeta, että vastaajat suhtautuvat yksityisen tiedon jakamiseen melko löyhästi ja huolettomasti eivätkä usko vakoiluohjelmien tuomaan todelliseen vaaraan, asenteet muuttuvat luultavasti ainoastaan kantapään kautta. Yksinkertaisena ohjeena voikin pitää; Mieti ja lue tarkkaan mitä lataat ja mille annat luvan.

Teoriaosuutta koottaessa törmäsin aiemmin oletettuun asiaan. Tutkimuksen aiheesta, vakoiluohjelmista mobiililaitteissa, on hyvin haastavaa löytää luotettavaa ja kattavaa tietoa. Haku eri painettuihin tietokantoihin hakusanoilla ”mobiililaite”, ”haittaohjelma” ja ”vakoiluohjelma” eivät tuottaneet käytännössä minkäänlaista tulosta. Teoriaosuus tulikin koota yksittäisten internet -lähteiden varaan. Toisaalta näitä lähteitä oli melko hyvin saatavilla. Kahden alan ammattilaisen haastattelemisen mukaan ottaminen oli erinomainen lisä tutkimukselle, erityisesti F-Securen Albrechtin vastaukset antoivat vahvistusta ja lisätukea koko prosessille. Oli myös oikea päätös rajata tutkimustyö yksityiskäytössä oleviin mobiililaitteisiin, sillä niille mobiililaitteille on täysin ”omat” vakoiluohjelmat, kun verrataan esimerkiksi työkäytössä oleviin laitteisiin.

5.2 Tutkimustuloksien luotettavuus

Kyselyn tuloksia voidaan pitää kohtuullisen luotettavina. Ei ole syytä epäillä, etteivätkö vastaajat olisi vastanneet kyselyyn rehellisesti ja todenmukaisesti. Vastauksia saatiin kohtuullinen määrä, joskin hieman epätasaisesti sukupuolta ja ikää tarkasteltaessa. Vaikkakin luotettavuuden kannalta suurempi vastausmäärä ei olisi ollut pahitteeksi, päättelisin mobiililaitteiden käyttäjien olevan saatujen vastusten perusteelta käytöltään melko ”tasaista massaa”. Vastaajat käyttivät melko samoja, suosituimpia laitteita ja samoja suosittuja sovelluksia.

5.3 Tutkimuksen eettisyys

Tutkimuksessa on mielestäni toimittu hyvän etiikan mukaisesti. Vastaajat tiesivät huolellisen saatteen ansiosta, mihin osallistuivat. Kysymykset oli pyritty laatimaan mahdollisimman selkeiksi ja niissä pyrittiin välttämään valmiita oletuksia. Vastaukset on käsitelty todenmukaisesti ja raportoitu mahdollisimman kattavasti, erilaisten kuvioiden ja taulukoiden kera.

5.4 Opinnäytetyöprosessi

Opinnäytetyö on ollut minulle opettava prosessi. Useasti oli palattava taaksepäin, jotta seuraavan askeleen pystyi ottamaan aiempaa edemmäs. Prosessi on opettanut minulle perustavanlaatuista tutkimustyötä ja erityisesti sen, että huolellinen suunnittelu ja suunnitelma ovat jo puoli voittoa. Prosessi on opettanut myös sen, että tutkittavaan asiaan perehtyminen, lähteiden kartoitus ja kyselyn ja haastattelujen laatiminen vievät paljon aikaa. Itse kirjoittaminen on ollut yllättävän pieni osuus opinnäytetyön prosessista.

5.5 Jatkotutkimusehdotukset

Aihe itsessään on hyvin laaja. Jatkotutkimuksena voisi perehtyä tarkemmin jonkin tietyn laitteen ja sen käyttäjien toimintaan. Esimerkiksi Android käyttäjiin, siltä osin, kun Androidia pidetään yleisimmin haavoittuvimpana mobiililaitteiden käyttöjärjestelmänä. Jatkotutkimusehdotuksena antaisin myös tietokartoituksen aiheeseen liittyen, minkä verran ja millä hakusanoilla löytyy tietoa aiheesta, niin painetuista kuin sähköisistä tietokannoista. Kolmas ehdotus olisi ottaa selvää sellaisten mobiililaitteiden käyttäjien kokemuksia, joiden laitteessa on ollut vakoiluohjelma. Mahdollisesti sellaisten kokemusten, joissa käyttäjä on kokenut selvästi suurempaa haittaa, esilletuonti voisi toimia riskien tietoisuutta lisäävänä tekijänä.

Lähteet

AV-Test, 01/2016, av-test.org, The best antivirus software for Android
Luettavissa: https://www.av-test.org/en/antivirus/mobile-devices/
Luettu: 08.04.2016

It-viikko, 06/2014, itviikko.fi, Tätä on ”laillinen” vakoilu: Koko puhelin kaapataan
Luettavissa: http://www.itviikko.fi/uutiset/2014/06/26/tata-on-laillinen-vakoilu-koko-puhelin-kaapataan/20148947/7
Luettu: 26.03.2016

Kovamäki, P., 2007, wiki.tut.fi, Haittaohjelmat mobiililaitteissa
Luettavissa: https://wiki.tut.fi/Tietoturva/Tutkielmat/2007-24
Luettu: 26.03.2016

Lillbacka, J., 02/2012, thesus.fi, Informaatiosodankäynti – tietoverkkojen vaarat
Luettavissa:
https://www.theseus.fi/bitstream/handle/10024/43303/Lillbacka_Juhani.pdf?sequence=1
Luettu 26.03.2016 s.30

Lehtonen, T., 08/2012, ts.fi, Vakoiluohjelma ottaa kännykän haltuunsa
Luettavissa:
http://www.ts.fi/uutiset/ulkomaat/384509/Vakoiluohjelma+ottaa+kannykan+haltuunsa
Luettu: 27.03.2016

Mobilespyonline, 01/2013, mobilespyonline.com, Lataa ilmainen vakoiluohjelmien koskematta kohdepuhelimeen
Luettavissa: http://mobilespyonline.com/fi/ladata-ilmaiseksi-spyware-koskematta-kohdepuhelimeen/
Luettu: 26.03.2016

Norton, securityresponse.symantec.com, Opettele tuntemaan vakoiluohjelmien lukuisat tavoitteet
Luettavissa:
http://securityresponse.symantec.com/fi/fi/norton/products/library/article.jsp?aid=catch_spyware_before#360
Luettu: 26.03.2016

Norton, 07/2013, norton.com, Älypuhelimien mobiilipalvelujen turvallisuuden varmistaminen
Luettavissa: http://fi.norton.com/mobile-safety/article
Luettu: 27.03.2016

Pitkänen, P., 11/2011, iltasanomat.fi, Tutkija: Miljoonissa Android- ja Nokia-puhelimissa on vakoiluohjelma
Luettavissa: http://www.iltasanomat.fi/digi/art-2000000454187.html
Luettu: 27.03.2016

Suomen Mobiiliasiantuntijat, 05/2015, mobiiliasiantuntijat.fi, Mobiilitietoturvavinkkejä kuluttajille ja pienille organisaatioille
Luettavissa: http://www.mobiiliasiantuntijat.fi/mobiilitietoturvavinkit.html
Luettu: 27.03.2016

Taloussanomat, 02/2008, digitoday.fi, Puheluita on helppo salakuunnella
Luettavissa: http://www.digitoday.fi/tietoturva/2008/02/08/puheluita-on-helppo-salakuunnella/20083948/66
Luettu: 01.04.2016

Taloussanomat, 22.05.2012, Apple ei anna kehittää virustorjuntaa iPhoneen
Luettavissa: http://www.digitoday.fi/tietoturva/2012/05/22/apple-ei-anna-kehittaa-virustorjuntaa-iphoneen/201229894/66
Luettu: 08.04.2016

Tietoturvapalvelu, tietoturvapalvelu.info, Haittaohjelmat ja muut uhat
Luettavissa: http://www.tietoturvapalvelu.info/johdanto/haittaohjelmat_ja_muut_uhat
Luettu: 01.04.2016

Yle, 05/2015, yle.fi/uutiset, Mustasukkaisille myydään kännyköiden vakoiluohjelmia
Luettavissa:
http://yle.fi/uutiset/mustasukkaisille_myydaan_kannykoiden_vakoiluohjelmia/5238418
Luettu: 26.03.2016

Vali, K., 03/2016, puhelinjaluuri.teknologiaforum.com, Category Archives: Myydyimmät Puhelimet
Luettavissa: http://www.puhelinjaluuri.teknologiaforum.com/?cat=29
Luettu: 26.03.2016

Liitteet

Liite 1. Kyselylomakkeen saate

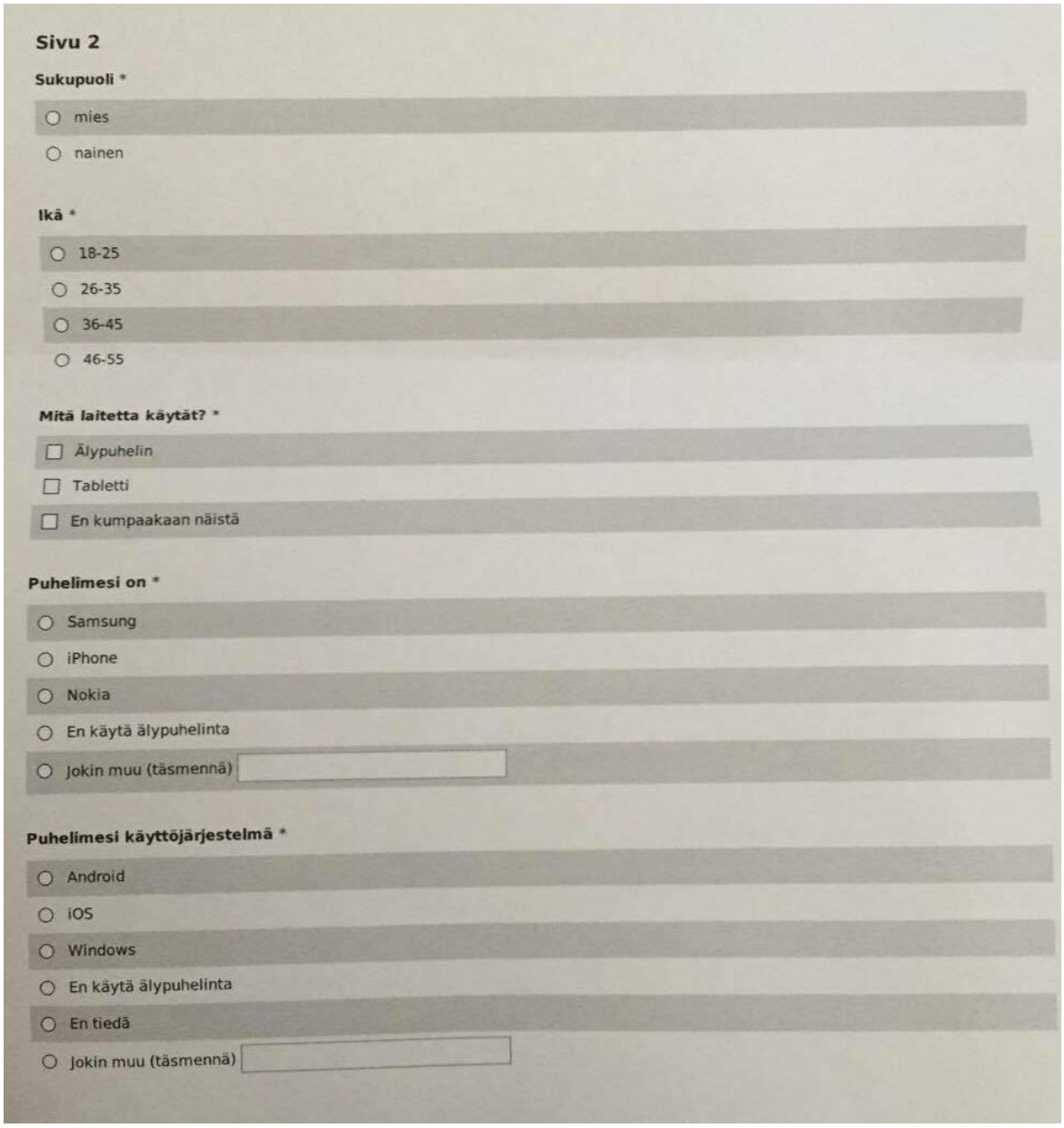
Hyvä vastaaja

Opiskelen Pasilan Haaga-Helian ammattikorkeakoulussa tradenomin tutkintoon johtavassa koulutuksessa. Tutkin opinnäytetyössäni vakoiluohjelmien tunnettavuutta suomalaisten keskuudessa. Osana opinnäytetyötäni on tämä kysely, johon pyydän teitä osallistumaan. Kyselyyn osallistuminen tarkoittaa oheisen kyselylomakkeen täyttämistä. Osallistuminen on vapaaehtoista, kyselyyn vastaamisen voi keskeyttää missä vaiheessa tahansa.

Kyselyyn osallistuminen on täysin luottamuksellista. Tutkimuksen tekemiseen on saatu asianmukainen lupa. Antamanne vastaukset käsitellään nimettöminä ja ehdottaman luottamuksellisesti. Kenenkään vastaajan tiedot eivät paljastu tuloksissa. Kyselyyn vastaamiseen on aikaa kaksi viikkoa.

Vastauksesta kiittäen,
Egle Kuivaniemi, opiskelija

Liite 2. Kyselylomake



Sivu 2

Sukupuoli *

- ○ mies
- ○ nainen

Ikä *

- ○ 18-25
- ○ 26-35
- ○ 36-45
- ○ 46-55

Mitä laitetta käytät? *

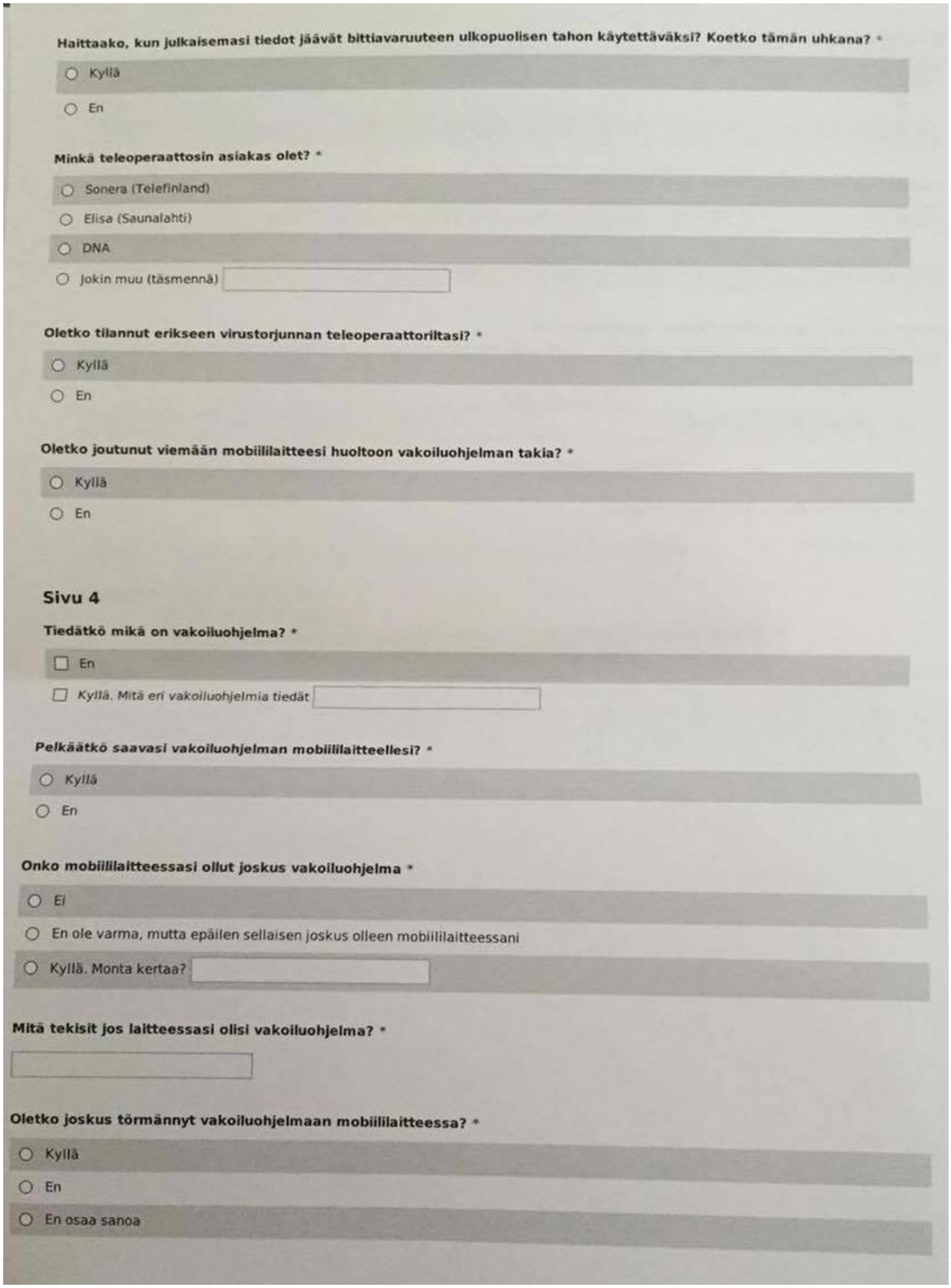
- ☐ Älypuhelin
- ☐ Tabletti
- ☐ En kumpaakaan näistä

Puhelimesi on *

- ○ Samsung
- ○ iPhone
- ○ Nokia
- ○ En käytä älypuhelinta
- ○ Jokin muu (täsmennä)

Puhelimesi käyttöjärjestelmä *

- ○ Android
- ○ iOS
- ○ Windows
- ○ En käytä älypuhelinta
- ○ En tiedä
- ○ Jokin muu (täsmennä)



Haittaako, kun julkaisemasi tiedot jäävät bittiavaruuteen ulkopuolisen tahon käytettäväksi? Koetko tämän uhkana? *

- ○ Kyllä
- ○ En

Minkä teleoperaattosin asiakas olet? *

- ○ Sonera (Telefinland)
- ○ Elisa (Saunalahti)
- ○ DNA
- ○ Jokin muu (täsmennä)

Oletko tilannut erikseen virustorjunnan teleoperaattoriltasi? *

- ○ Kyllä
- ○ En

Oletko joutunut viemään mobiililaitteesi huoltoon vakoiluohjelman takia? *

- ○ Kyllä
- ○ En

Sivu 4

Tiedätkö mikä on vakoiluohjelma? *

- ☐ En
- ☐ *Kyllä. Mitä eri vakoiluohjelmia tiedät*

Pelkäätkö saavasi vakoiluohjelman mobiililaitteellesi? *

- ○ *Kyllä*
- ○ *En*

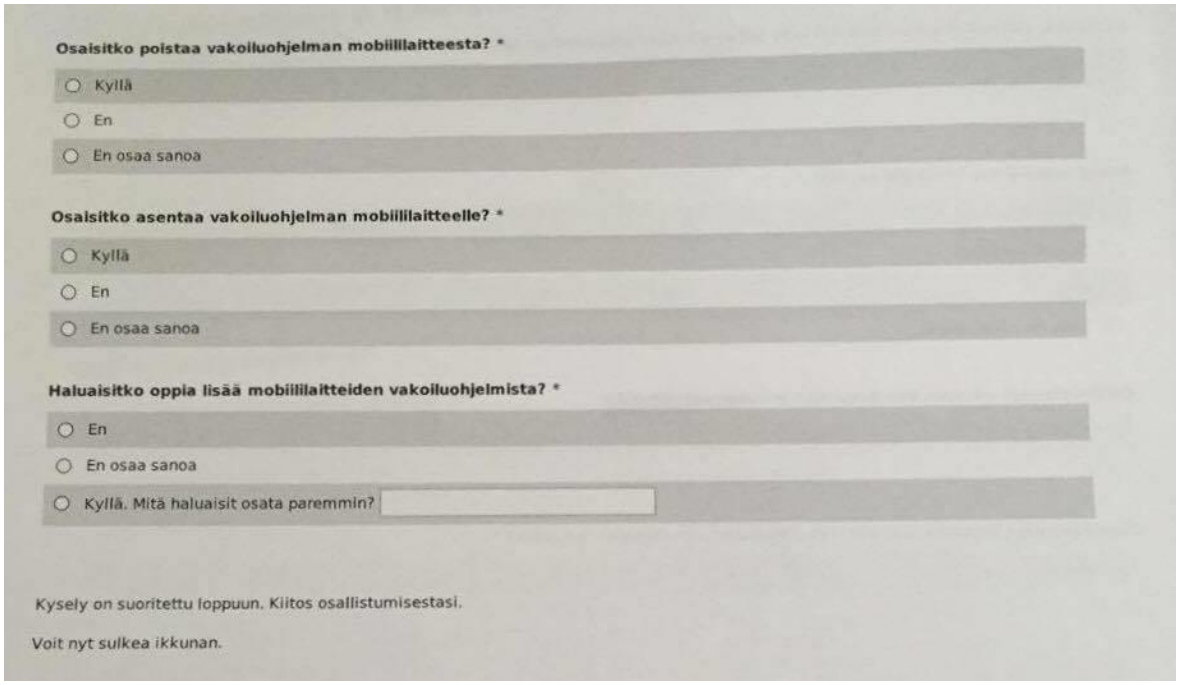
Onko mobiililaitteessasi ollut joskus vakoiluohjelma *

- ○ *Ei*
- ○ En ole varma, mutta epäilen sellaisen joskus olleen mobiililaitteessani
- ○ Kyllä. Monta kertaa?

Mitä tekisit jos laitteessasi olisi vakoiluohjelma? *

Oletko joskus törmännyt vakoiluohjelmaan mobiililaitteessa? *

- ○ Kyllä
- ○ En
- ○ En osaa sanoa



Osaisitko poistaa vakoiluohjelman mobiililaitteesta? *

- ○ Kyllä
- ○ En
- ○ En osaa sanoa

Osaisitko asentaa vakoiluohjelman mobiililaitteelle? *

- ○ Kyllä
- ○ En
- ○ En osaa sanoa

Haluaisitko oppia lisää mobiililaitteiden vakoiluohjelmista? *

- ○ En
- ○ En osaa sanoa
- ○ Kyllä. Mitä haluaisit osata paremmin?

Kysely on suoritettu loppuun. Kiitos osallistumisestasi.

Voit nyt sulkea ikkunan.

Liite 3. Saatekirje haastattelulle

Hyvä vastaaja!

Olen it-tradenomiopiskelija Haaga-Helian ammattikorkeakoulusta. Olen kirjoittamassa ja työstämässä opinnäytetyötäni ja pyytäisin saada luvan haastatella Teitä. Työni tarkoitus on selvittää miten paljon Suomen väestö tietää vakoiluohjelmista ja miten paljon siitä on tietoa saatavilla noin yleisellä tasolla.

Lähettäisin haastattelun teille word- asiakirjana ja toivoisin, että sen täytettyänne lähettäisitte sen minulle takaisin sähköisesti. Tutkimukseen osallistuminen on täysin vapaaehtoista, pyytäisin Teiltä vain hetken aikaanne täyttääksenne haastattelun kysymykset.

Kiittäen Teitä jo etukäteen yhteistyöstä!

Ystävällisin terveisin,
Egle Kuivaniemi, egle.petaja@hotmail.com

Liite 4. Haastattelulomake Elisa-myymälälle

Haastattelu	opinnäytetyölle Vakoiluohjelmat Mobiililaitteissa
Haastattelija: Egle Kuivaniemi	Haaga-Helian opiskelija
Vastaaja: Marko Petäjä	myymäläpäällikkö
26.03.2016 Forssa	

- Kauanko olet ollut Elisalla töissä?

- Kuinka yleisiä virukset ovat mobiililaitteissa nykypäivänä?

- Osaisitko erotella, kuinka suuri osuus näistä on vakoiluohjelmilla?

- Kuinka usein kohtaat asiakkaita jotka epäilevät mobiililaitteessaan olevan jokin vakoiluohjelma?

- Menevätkö virustorjunnat usein kaupaksi mobiililaitteiden ostajille?

Liite 5. Haastattelulomake F-Secure yhtiölle

Haastattelu	opinnäytetyölle Vakoiluohjelmat Mobiililaitteissa
Haastattelija: Egle Kuivaniemi	Haaga-Helian opiskelija
Vastaaja: Mikael Albrecht	Security Specialist
07.04.2016 Helsinki	

- Kuinka yleisiä virukset ovat mobiililaitteissa nykypäivänä?
- Osaisitko erotella, kuinka suuri osuus näistä on vakoiluohjelmilla?
- Kuinka usein kohtaat asiakkaita, jotka epäilevät mobiililaitteessaan olevan jokin vakoiluohjelma? Vai hoitavatko yleensä operaattorit nämä asiat huollon kanssa, teille asti ei siis tieto tulisi?
- Yleisesti ottaen kuinka vaikeaa on vakoiluohjelman poistaminen mobiililaitteesta?
- Menevätkö virustorjunnat usein kaupaksi mobiililaitteiden ostajille?
- Mitä kaikkia tietoja vakoiluohjelmat yleensä keräävät mobiililaitteista? Vai onko se enemmän vakoiluohjelmakohtaista?
- Esiintyykö joillain tietyillä tuotemerkeillä toisia enemmän vakoiluohjelmia?